Den Europæiske Unions

Tidende

L 44

Dansk udgave

Retsforskrifter

65. årgang

24. februar 2022

Indhold

[1] EØS-relevant tekst.

II

(Ikke-lovgivningsmæssige retsakter)

AFGØRELSER

KOMMISSIONENS GENNEMFØRELSESAFGØRELSE (EU) 2022/254

af 17. december 2021

i henhold til Europa-Parlamentets og Rådets forordning (EU) 2016/679 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Republikken Korea i henhold til lov om beskyttelse af personoplysninger

(meddelt under nummer C(2021) 9316)

(EØS-relevant tekst)

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) ([1]), særlig artikel 45, stk. 3,

ud fra følgende betragtninger:

1. INDLEDNING

(1) I forordning (EU) 2016/679 fastsættes reglerne for overførsel af personoplysninger fra en dataansvarlig eller databehandler i Unionen til tredjelande og internationale organisationer, i det omfang overførslen falder inden for forordningens anvendelsesområde. Reglerne om internationale dataoverførsler er fastsat i kapitel V (artikel 44-50) i nævnte forordning. Strømmen af personoplysninger til og fra lande uden for Den Europæiske Union er afgørende for udvidelsen af den grænseoverskridende handel og det internationale samarbejde, men niveauet for beskyttelse af personoplysninger i Unionen må ikke undermineres af overførsler til tredjelande ([2]).

(2) I henhold til artikel 45, stk. 3, i forordning (EU) 2016/679 kan Kommissionen ved hjælp af en gennemførelsesretsakt fastslå, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland eller en international organisation sikrer et tilstrækkeligt beskyttelsesniveau. På denne betingelse kan overførsel af personoplysninger til et tredjeland finde sted uden yderligere godkendelse, jf. artikel 45, stk. 1, og betragtning 103 i forordning (EU) 2016/679.

(3) Som omhandlet i artikel 45, stk. 2, i forordning (EU) 2016/679 skal vedtagelsen af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet finde sted på grundlag af en omfattende analyse af det pågældende tredjelands retsorden, både hvad angår de regler, der finder anvendelse på dataimportøren, og de begrænsninger og garantier, der gælder med hensyn til offentlige myndigheders adgang til personoplysninger. I sin vurdering skal Kommissionen fastslå, om det pågældende tredjeland sikrer et beskyttelsesniveau, som »i det væsentlige svarer« til det, der sikres i Den Europæiske Union (betragtning 104 i forordning (EU) 2016/679). Om dette er tilfældet, skal vurderes i forhold til EU-lovgivningen, navnlig forordning (EU) 2016/679, samt Den Europæiske Unions Domstols retspraksis ([3]).

([1]) EUT L 119 af 4.5.2016, s. 1.
([2]) Jf. betragtning 101 i forordning (EU) 2016/679.
([3]) Se senest sag C-311/18, Facebook Ireland og Schrems (»Schrems II«), ECLI:EU:C:2020:559.

(4) Som Den Europæiske Unions Domstol har præciseret, kræves der ikke et identisk beskyttelsesniveau ([4]). Det betyder navnlig, at de midler, som tredjelandet anvender til at beskytte personoplysninger, kan være forskellige fra de midler, som anvendes inden for Unionen, så længe de i praksis viser sig at være effektive med henblik på at sikre et tilstrækkeligt beskyttelsesniveau ([5]). Standarden for tilstrækkelighed er derfor ikke, at EU-reglerne duplikeres afsnit for afsnit. Testen består snarere i, om det pågældende udenlandske system som helhed sikrer det krævede beskyttelsesniveau gennem kerneindholdet i retten til privatlivets fred og den effektive gennemførelse, overvågning og håndhævelse heraf ([6]). Det Europæiske Databeskyttelsesråds reference vedrørende et tilstrækkeligt beskyttelsesniveau, der skal præcisere denne standard yderligere, giver også vejledning i denne henseende ([7]).

(5) Kommissionen har foretaget en grundig analyse af den koreanske lovgivning og praksis. På grundlag af konklusionerne i betragtning 8-208 konkluderer Kommissionen, at Republikken Korea sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger, der overføres fra en dataansvarlig eller databehandler i Unionen ([8]) til enheder (f.eks. fysiske eller juridiske personer, organisationer, offentlige institutioner) i Korea, der er omfattet af anvendelsesområdet for lov om beskyttelse af personoplysninger (lov nr. 10465 af 29. marts 2011, senest ændret ved lov nr. 16930 af 4. februar 2020). Dette omfatter både dataansvarlige og databehandlere (såkaldte »outsourcingpartnere« ([9])) som omhandlet i forordning (EU) 2016/679. Konstateringen af et tilstrækkeligt beskyttelsesniveau omfatter ikke behandling af personoplysninger i forbindelse med religiøse organisationers missionsarbejde og politiske partiers udnævnelse af kandidater eller behandling af personlige kreditoplysninger i medfør af lov om kreditoplysninger foretaget af dataansvarlige underlagt kommissionen for finansielle tjenesteydelsers tilsyn.

(6) I denne konklusion tages der hensyn til de yderligere garantier, der er fastsat i meddelelse nr. 2021-5 (bilag I), og de officielle redegørelser, forsikringer og tilsagn fra den koreanske regering til Kommissionen (bilag II).

(7) Denne afgørelse har den virkning, at overførsler til dataansvarlige og databehandlere i Republikken Korea kan finde sted, uden at der behøves yderligere tilladelse. Den berører ikke den direkte anvendelse af forordning (EU) 2016/679 på sådanne enheder, hvis betingelserne vedrørende forordningens territoriale anvendelsesområde, jf. forordningens artikel 3, er opfyldt.

2. REGLERNE FOR BEHANDLING AF PERSONOPLYSNINGER

2.1. Databeskyttelsesrammen i Republikken Korea

(8) Den retlige ordning for beskyttelse af privatlivets fred og databeskyttelse i Korea har sine rødder i den koreanske forfatning, som blev bekendtgjort den 17. juli 1948. Selv om retten til beskyttelse af personoplysninger ikke udtrykkeligt er fastsat i forfatningen, anerkendes den ikke desto mindre som en grundlæggende rettighed, der udspringer af de forfatningsmæssige rettigheder til menneskelig værdighed og stræben efter lykke (artikel 10), privatliv (artikel 17) og privatlivets fred i forbindelse med kommunikation (artikel 18). Dette er blevet bekræftet af både højesteret ([10]) og forfatningsdomstolen ([11]). Begrænsninger af grundlæggende rettigheder og friheder (herunder retten til privatlivets fred) kan kun pålægges ved lov, når det er nødvendigt af hensyn til den nationale sikkerhed eller opretholdelsen af lov og orden og den offentlige velfærd, og må ikke berøre den pågældende rettigheds eller friheds væsentligste indhold (artikel 37, stk. 2).

([4]) Sag C-362/14, Maximilian Schrems mod Data Protection Commissioner (»Schrems«), ECLI:EU:C:2015:650, præmis 73.
([5]) Schrems, præmis 74.
([6]) Jf. meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om udveksling og beskyttelse af personoplysninger i en globaliseret verden, COM(2017) 7 af 10.1.2017, afsnit 3.1., s. 6.
([7]) Det Europæiske Databeskyttelsesråd, Adequacy Referential, WP 254 rev. 01. Kan findes på følgende link: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108.
([8]) Denne afgørelse er EØS-relevant. I henhold til aftalen om Det Europæiske Økonomiske Samarbejdsområde (EØS-aftalen) udvides Den Europæiske Unions indre marked til at omfatte de tre EØS-stater Island, Liechtenstein og Norge. Det Blandede EØS-Udvalgs afgørelse om indarbejdelse af forordning (EU) 2016/679 i bilag XI til EØS-aftalen blev vedtaget af Det Blandede EØS-Udvalg den 6. juli 2018 og trådte i kraft den 20. juli 2018. Forordningen er således omfattet af nævnte aftale. I forbindelse med afgørelsen skal henvisninger til EU og EU-medlemsstaterne således forstås således, at de også omfatter EØS-staterne.
([9]) Jf. afsnit 2.2.3 i denne afgørelse.
([10]) Jf. f.eks. højesterets afgørelse 2014Da77970 af 15. oktober 2015 (engelsk resumé findes under linket »Lawmaker's disclosure of teachers' trade union members case« på https://www.privacy.go.kr/eng/enforcement_01.do) og den deri nævnte retspraksis, herunder afgørelse 2012Da49933 af 24. juli 2014.
([11]) Jf. navnlig forfatningsdomstolens afgørelse nr. 99Hun-ma513 af 26. maj 2005 (engelsk resumé findes på http://www.koreanlii.or.kr/w/index.php/99Hun-Ma513?ckattempt=2) og afgørelse nr. 2014JHun-ma449 2013 Hun-Ba68 (konsolideret) af 23. december 2015 (engelsk resumé findes under linket »Change of resident registration number case« på https://www.privacy.go.kr/eng/enforcement_01.do).

(9) Selv om forfatningen flere steder henviser til koreanske statsborgeres rettigheder, har forfatningsdomstolen fastslået, at udenlandske statsborgere også har grundlæggende rettigheder ([12]). Domstolen har navnlig fastslået, at beskyttelsen af ens værdighed og værdi som menneske samt retten til at søge lykke er rettigheder, der tilkommer ethvert menneske og ikke blot statsborgere ([13]). Ifølge den koreanske regerings officielle redegørelser ([14]) er det desuden almindeligt anerkendt, at der i forfatningens artikel 12-22 (som omfatter retten til privatlivets fred) er fastsat grundlæggende menneskerettigheder ([15]). Selv om der indtil videre ikke findes nogen retspraksis, som specifikt vedrører udenlandske statsborgeres ret til privatlivets fred, understøtter dens forankring i beskyttelsen af den menneskelige værdighed og stræben efter lykke denne konklusion ([16]).

(10) Desuden har Korea vedtaget en række love på databeskyttelsesområdet, som indeholder garantier for alle personer, uanset deres nationalitet ([17]). I forbindelse med denne afgørelse er de relevante love:

— lov om beskyttelse af personoplysninger (PIPA)

— lov om anvendelse og beskyttelse af kreditoplysninger ([18])

— lov om beskyttelse af privatlivets fred i forbindelse med kommunikation.

(11) PIPA udgør den generelle retlige ramme for databeskyttelse i Republikken Korea. Den suppleres af et gennemførelsesdekret (præsidentielt dekret nr. 23169 af 29. september 2011, senest ændret ved præsidentielt dekret nr. 30892 af 4. august 2020) (PIPA-gennemførelsesdekretet), der i lighed med PIPA er retligt bindende og kan håndhæves.

(12) Desuden indeholder lovgivningsmæssige »meddelelser« vedtaget af kommissionen for beskyttelse af personoplysninger (PIPC eller beskyttelseskommissionen) supplerende regler for fortolkning og anvendelse af PIPA. På grundlag af artikel 5 (statslige forpligtelser) og artikel 14 (internationalt samarbejde) i PIPA vedtog PIPC meddelelse nr. 2021-5 af 1. september 2020 (som ændret ved meddelelse nr. 2021-1 af 21. januar 2021 og meddelelse nr. 2021-5 af 16 november 2021, i det følgende meddelelse nr. 2021-5) om fortolkning, anvendelse og håndhævelse af visse bestemmelser i PIPA. Denne meddelelse indeholder præciseringer, der finder anvendelse på enhver behandling af personoplysninger under PIPA, samt supplerende garantier for personoplysninger, der overføres til Korea på grundlag af denne afgørelse. Meddelelsen er juridisk bindende for de persondataansvarlige og kan både håndhæves af PIPC og domstolene ([19]). En overtrædelse af reglerne i meddelelsen indebærer en overtrædelse af de relevante bestemmelser i PIPA, som de supplerer. Indholdet af de supplerende garantier analyseres derfor som led i vurderingen af de relevante PIPA-artikler. Endelig er der yderligere vejledning om PIPA og gennemførelsesdekretet hertil, som danner grundlag for PIPC's anvendelse og håndhævelse af databeskyttelsesreglerne, i PIPC's PIPA-håndbog og -retningslinjer ([20]).

([12]) Forfatningsdomstolens afgørelse nr. 93 Hun-MA120 af 29. december 1994.
([13]) Forfatningsdomstolens afgørelse nr. 99HeonMa494 af 29. november 2001.
([14]) Jf. afsnit 1.1 i bilag II.
([15]) Se også artikel 1 i lov om beskyttelse af personoplysninger, hvori der udtrykkeligt henvises til »den enkeltes friheder og rettigheder«. Mere specifikt hedder det, at formålet med en sådan lov er »at sikre behandling og beskyttelse af personoplysninger med henblik på at beskytte den enkeltes friheder og rettigheder og styrke den enkeltes værdighed og værdi.« I artikel 5, stk. 1, i lov om beskyttelse af personoplysninger fastslås det på samme måde, at staten har til opgave at »formulere politikker til forebyggelse af skadelige konsekvenser af indsamling, misbrug og forkert anvendelse af personoplysninger, indiskret overvågning og sporing mv. og til styrkelse af den enkeltes værdighed og ret til privatlivets fred.«
([16]) Endvidere bestemmer forfatningens artikel 6, stk. 2, at udenlandske statsborgeres status er garanteret i overensstemmelse med folkeretten og internationale traktater. Korea er part i flere internationale aftaler, der garanterer retten til privatlivets fred, såsom den internationale konvention om borgerlige og politiske rettigheder (artikel 17), konventionen om rettigheder for personer med handicap (artikel 22) og konventionen om barnets rettigheder (artikel 16).
([17]) Dette omfatter regler, der er relevante for beskyttelsen af personoplysninger, men som ikke finder anvendelse i en situation, hvor personoplysninger indsamles i Unionen og overføres til Korea i henhold til forordning (EU) 2016/679, f.eks. i lov om beskyttelse, anvendelse mv. af lokaliseringsdata.
([18]) Formålet med denne lov er at fremme en sund kreditoplysningsvirksomhed, fremme en effektiv anvendelse og systematisk forvaltning af kreditoplysninger og beskytte privatlivets fred mod forkert anvendelse og misbrug af kreditoplysninger (lovens artikel 1).
([19]) Koreanske domstole har f.eks. truffet afgørelse om overholdelse af lovgivningsmæssige meddelelser i en række sager, herunder ved at holde koreanske dataansvarlige ansvarlige for overtrædelser af en meddelelse (jf. f.eks. højesterets afgørelse 2018Da219406 af 25. oktober 2018, hvor domstolen pålagde en dataansvarlig at betale erstatning til enkeltpersoner for skade som følge af en overtrædelse af meddelelsen om standarden for foranstaltninger til at garantere personoplysningers sikkerhed, se også højesterets afgørelse 2018Da219352 af 25. oktober 2018, højesterets afgørelse 2011Da24555 af 16. maj 2016, distriktsdomstolen i Seouls afgørelse 2014Gahap511956 af 13. oktober 2016, distriktsdomstolen i Seouls afgørelse 2009Gahap43176 af 26. januar 2010.
([20]) Artikel 12, stk. 1, i PIPA.

(13) Desuden indeholder lov om anvendelse og beskyttelse af kreditoplysninger (CIA) specifikke regler, der gælder både for »almindelige« kommercielle operatører og specialiserede enheder i den finansielle sektor, der behandler personlige kreditoplysninger, dvs. oplysninger, der er nødvendige for at fastslå kreditværdigheden af parter i finansielle eller kommercielle transaktioner. Dette omfatter navnlig navn, kontaktoplysninger, finansielle transaktioner, kreditvurdering, forsikringsstatus eller lånebalance, når sådanne oplysninger anvendes til at fastslå en persons kreditværdighed ([21]). Når sådanne oplysninger anvendes til andre formål (f.eks. menneskelige ressourcer), finder PIPA derimod anvendelse i sin helhed. Med hensyn til de specifikke databeskyttelsesbestemmelser i CIA overvåges overholdelsen dels af PIPC (for kommercielle organisationer, jf. artikel 45-3 i CIA), dels af kommissionen for finansielle tjenesteydelser ([22]) (for finanssektoren, herunder kreditvurderingsbureauer, banker, forsikringsselskaber, sparekasser, specialiserede kreditfinansieringsselskaber, finansielle investeringsselskaber, værdipapirfinansieringsselskaber, kreditforeninger osv., jf. artikel 45, stk. 1, i CIA sammenholdt med artikel 36-2 i CIA-gennemførelsesdekretet og artikel 38 i lov om kommissionen for finansielle tjenesteydelser). I denne forbindelse er anvendelsesområdet for denne afgørelse begrænset til kommercielle operatører, der er underlagt PIPC's tilsyn ([23]). De specifikke regler i CIA, der finder anvendelse i denne forbindelse (de generelle regler i PIPA finder anvendelse, hvis der ikke findes specifikke regler), er beskrevet i afsnit 2.3.11.

2.2. **PIPA's materielle og personelle anvendelsesområde**

(14) Medmindre andet er fastsat udtrykkeligt i andre retsakter, er beskyttelsen af personoplysninger omfattet af PIPA (artikel 6). Det materielle og personelle anvendelsesområde bestemmes af de definerede begreber »personoplysninger«, »behandling« og »persondataansvarlig«.

2.2.1. *Definition af personoplysninger*

(15) I artikel 2, stk. 1, i PIPA defineres personoplysninger som oplysninger om en levende person, der identificerer den pågældende direkte, f.eks. ved dennes navn, bopælsregistreringsnummer eller billede, eller indirekte, dvs. når oplysninger, der ikke i sig selv kan identificere en bestemt person, let kan samkøres med andre oplysninger. Om oplysningerne »let« kan samkøres, afhænger af, om en sådan samkøring med rimelighed er sandsynlig under hensyntagen til muligheden for at indhente andre oplysninger samt til den tid, de omkostninger og den teknologi, der er nødvendig for at identificere en person.

(16) Desuden betragtes pseudonymiserede oplysninger — dvs. oplysninger, der ikke kan identificere en bestemt person uden at bruge eller samkøre oplysningerne med supplerende oplysninger for at genoprette dem til deres oprindelige tilstand — som personoplysninger i henhold til PIPA (artikel 2, stk. 1, litra c), i PIPA). Omvendt er oplysninger, der er fuldt ud »anonymiserede«, udelukket fra PIPA's anvendelsesområde (artikel 58-2 i PIPA). Dette gælder oplysninger, der ikke kan identificere en bestemt person, selv om de samkøres med andre oplysninger, under hensyntagen til den tid, de omkostninger og den teknologi, der med rimelighed er nødvendig til identifikation.

(17) Dette svarer til det materielle anvendelsesområde for forordning (EU) 2016/679 og dens begreber »personoplysninger«, »pseudonymisering« ([24]) og »anonymiserede oplysninger« ([25]).

([21]) Artikel 2, stk. 1, i CIA.

([22]) Kommissionen for finansielle tjenesteydelser er Koreas tilsynsmyndighed for den finansielle sektor og håndhæver i denne egenskab også CIA.

([23]) Hvis dette ændres i fremtiden, f.eks. ved at udvide PIPC's kompetenceområde til al behandling af personlige kreditoplysninger omfattet af CIA, kan det overvejes at ændre afgørelsen om tilstrækkeligheden af beskyttelsesniveauet, så den også omfatter de enheder, der i øjeblikket er underlagt kommissionen for finansielle tjenesteydelsers tilsyn.

([24]) I PIPA betragtes »pseudonymisering« som behandling ved brug af metoder såsom delvis sletning af personoplysninger eller delvis eller fuldstændig erstatning af personoplysninger på en sådan måde, at ingen specifik person kan genkendes uden supplerende oplysninger (artikel 2, stk. 1-2, i PIPA). Dette svarer til definitionen af pseudonymisering i artikel 4, stk. 5, i forordning (EU) 2016/679, som »behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person.«

([25]) Det præciseres navnlig i betragtning 26 i forordning (EU) 2016/679, at forordningen ikke bør gælde for anonyme oplysninger, dvs. oplysninger, der ikke vedrører en identificeret eller identificerbar fysisk person. Dette afhænger af alle de midler, der med rimelighed kan tænkes bragt i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere den pågældende. For at fastslå, om sådanne midler med rimelighed kan tænkes bragt i anvendelse, skal alle objektive forhold tages i betragtning såsom omkostninger ved og den tid, der er nødvendig til identifikation, under hensyntagen til den tilgængelige teknologi på behandlingstidspunktet og den teknologiske udvikling.

2.2.2. *Definition af behandling*

(18) Begrebet »behandling« defineres bredt i PIPA som »indsamling, frembringelse, sammenkobling, sammenkædning, registrering, opbevaring, værdiforøgende behandling, redigering, udtræk, output, berigtigelse, genoprettelse, anvendelse, fremlæggelse, videregivelse og tilintetgørelse af personoplysninger og andre lignende aktiviteter« ([26]). Selv om visse bestemmelser i PIPA kun henviser til bestemte typer behandling såsom »anvendelse«, »videregivelse« eller »indsamling« ([27]), fortolkes begrebet »anvendelse« således, at det omfatter enhver anden form for behandling end »indsamling« eller »videregivelse« (til tredjemand). Denne brede fortolkning af »anvendelse« sikrer således, at der ikke er huller i beskyttelsen i forbindelse med specifikke behandlingsaktiviteter. Begrebet behandling svarer derfor til det samme begreb i forordning (EU) 2016/679.

2.2.3. *Den persondataansvarlige og »outsourcingpartneren«*

(19) PIPA finder anvendelse på »persondataansvarlige« (den dataansvarlige). I lighed med i forordning (EU) 2016/679 omfatter dette enhver offentlig institution, juridisk person, organisation eller fysisk person, der behandler personoplysninger direkte eller indirekte med henblik på forvaltning af persondatafiler som led i deres aktiviteter ([28]). I denne forbindelse forstås ved »persondatafil« »et eller flere sæt personoplysninger, der er arrangeret eller organiseret på en systematisk måde på grundlag af en bestemt regel med henblik på let adgang til personoplysningerne« (artikel 2, stk. 4, i PIPA) ([29]). Internt er den dataansvarlige forpligtet til at uddanne de personer, der er involveret i behandlingen under dennes ledelse, f.eks. virksomhedsledere eller medarbejdere, og til at føre passende kontrol og tilsyn (artikel 28, stk. 1, i PIPA).

(20) Der gælder særlige forpligtelser, når den dataansvarlige (»outsourceren«) outsourcer behandlingen af personoplysninger til tredjemand (»outsourcingpartneren«). Outsourcingen skal navnlig være omfattet af en retligt bindende ordning (typisk en kontrakt) ([30]), som fastsætter omfanget af det outsourcede arbejde, formålet med behandlingen, de tekniske og forvaltningsmæssige garantier, der skal anvendes, den dataansvarliges tilsyn, erstatningsansvar (f.eks. erstatning for skade som følge af en overtrædelse af kontraktlige forpligtelser) samt begrænsningerne for enhver outsourcet databehandling ([31]) (artikel 26, stk. 1 og 2, i PIPA sammenholdt med artikel 28, stk. 1, i gennemførelsesdekretet) ([32]).

(21) Desuden skal den dataansvarlige offentliggøre og løbende ajourføre oplysninger om det outsourcede arbejde og outsourcingpartnerens identitet eller, i det omfang den outsourcede behandling vedrører direkte markedsføringsaktiviteter, underrette de berørte personer direkte om de relevante oplysninger (artikel 26, stk. 2 og 3, i PIPA sammenholdt med artikel 28, stk. 2-5, i gennemførelsesdekretet) ([33]).

(22) I henhold til artikel 26, stk. 4, i PIPA sammenholdt med artikel 28, stk. 6, i gennemførelsesdekretet er den dataansvarlige desuden forpligtet til at »uddanne« outsourcingpartneren i de nødvendige sikkerhedsforanstaltninger og føre tilsyn med, herunder gennem inspektioner, om outsourcingpartneren overholder alle den dataansvarliges forpligtelser i henhold til PIPA ([34]) og outsourcingkontrakten. Hvis outsourcingpartneren forvolder skade som følge af en overtrædelse af PIPA, gøres den dataansvarlige ansvarlig for outsourcingpartnerens handlinger eller undladelser med henblik på erstatningsansvar, som det er tilfældet med en ansat (artikel 26, stk. 6, i PIPA).

([26]) Artikel 2, stk. 2, i PIPA.
([27]) F.eks. henviser artikel 15-19 i PIPA kun til indsamling, anvendelse og videregivelse af personoplysninger
([28]) Artikel 2, stk. 5, i PIPA. Offentlige institutioner som omhandlet i PIPA omfatter alle centrale administrative myndigheder eller agenturer og deres tilknyttede organer, lokale myndigheder, skoler og lokale offentlige virksomheder, nationalforsamlingens forvaltningsorganer og retsvæsenet (herunder forfatningsdomstolen) (artikel 2, stk. 6, i PIPA sammenholdt med artikel 2 i PIPA-gennemførelsesdekretet).
([29]) Dette svarer til det materielle anvendelsesområde for forordning (EU) 2016/679. I henhold til artikel 2, stk. 1, i forordning (EU) 2016/679 finder forordningen anvendelse på »behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.« I artikel 4, nr. 6), i forordning (EU) 2016/679, defineres et register som »enhver struktureret samling af personoplysninger, der er tilgængelig efter bestemte kriterier«. I overensstemmelse hermed forklares det i betragtning 15, at beskyttelsen af personer bør gælde for »både automatisk og manuel behandling af personoplysninger, hvis personoplysningerne er indeholdt eller vil blive indeholdt i et register. Sagsmapper eller samlinger af sagsmapper samt deres forsider, som ikke er struktureret efter bestemte kriterier, bør ikke være omfattet af denne forordnings anvendelsesområde.«
([30]) Jf. PIPA-håndbogen, kapitel III, afsnit 2 om artikel 26 (s. 203-212), hvori det forklares, at artikel 26, stk. 1, i PIPA henviser til bindende ordninger såsom kontrakter eller lignende ordninger.
([31]) I henhold til artikel 26, stk. 5, i PIPA må databehandleren ikke anvende personoplysninger, der ikke er omfattet af det outsourcede arbejde, eller videregive personoplysninger til tredjemand. Manglende overholdelse af dette krav kan føre til strafferetlige sanktioner i henhold til artikel 71, nr. 2, i PIPA.
([32]) Manglende overholdelse af dette krav kan føre til pålæggelse af en bøde, jf. artikel 75, stk. 4, nr. 4, i PIPA.
([33]) Manglende overholdelse af dette krav kan føre til pålæggelse af en bøde, jf. artikel 75, stk. 2, nr. 1, og stk. 4, nr. 5, i PIPA.
([34]) Se også artikel 26, stk. 7, i PIPA, ifølge hvilken artikel 15-25, 27-31, 33-38 og 50 finder tilsvarende anvendelse på databehandleren.

(23) Selv om PIPA derfor ikke anvender forskellige begreber for »dataansvarlige« og »databehandlere«, omfatter reglerne om outsourcing i det væsentlige de samme forpligtelser og garantier som dem, der regulerer forholdet mellem dataansvarlige og databehandlere i henhold til forordning (EU) 2016/679.

2.2.4. *Særlige bestemmelser for udbydere af informations- og kommunikationstjenester*

(24) Selv om PIPA finder anvendelse på enhver dataansvarligs behandling af personoplysninger, indeholder visse bestemmelser specifikke regler (som en lex specialis) for »udbydere af informations- og kommunikationstjenesters« behandling af »brugeres« personoplysninger ([35]). Begrebet »brugere« omfatter personer, der anvender informations- og kommunikationstjenester (artikel 2, stk. 1, nr. 4, i lov om fremme af anvendelsen af informations- og kommunikationsnetværk og databeskyttelse, herefter netværksloven). Dette kræver, at vedkommende enten anvender teletjenester, der leveres af en koreansk teleoperatør, direkte, eller anvender informationstjenester ([36]), som leveres kommercielt (dvs. med gevinst for øje) af en enhed, der anvender tjenester fra en teleoperatør, som har licens/er registreret i Korea ([37]). I begge tilfælde er den enhed, der er bundet af de specifikke PIPA-bestemmelser, en enhed, der tilbyder en onlinetjeneste direkte til en person (dvs. en bruger).

(25) Omvendt vedrører en konstatering af et tilstrækkeligt beskyttelsesniveau udelukkende beskyttelsesniveauet for personoplysninger, der overføres fra en dataansvarlig/databehandler i Unionen til en enhed i et tredjeland (her: Republikken Korea). I sidstnævnte scenarie vil enkeltpersoner i Unionen normalt kun have en direkte forbindelse til »dataeksportøren« i Unionen og ikke til en koreansk udbyder af informations- og kommunikationstjenester ([38]). Derfor vil de særlige bestemmelser i PIPA vedrørende personoplysninger om brugere af informations- og kommunikationstjenester højst finde anvendelse i begrænsede situationer på personoplysninger, der overføres i henhold til denne afgørelse.

2.2.5. *Undtagelse fra visse bestemmelser i PIPA*

(26) Artikel 58, stk. 1, i PIPA udelukker anvendelsen af dele af PIPA (artikel 15-57) i forbindelse med fire kategorier af databehandling ([39]). De dele af PIPA, der omhandler de specifikke grunde til behandling, visse databeskyttelsesforpligtelser, de nærmere regler for udøvelsen af individuelle rettigheder samt reglerne for tvistbilæggelse i udvalget for bilæggelse af tvister om personoplysninger finder navnlig ikke anvendelse. Andre grundlæggende bestemmelser i PIPA finder fortsat anvendelse, navnlig de generelle bestemmelser om databeskyttelsesprincipper (artikel 3 i PIPA) — herunder f.eks. principperne om lovlighed, formålsspecificering og formålsbegrænsning, dataminimering, datanøjagtighed og -sikkerhed — og individuelle rettigheder (indsigt, berigtigelse, sletning og suspension, jf. artikel 4 i PIPA). Desuden pålægger artikel 58, stk. 4, i PIPA specifikke forpligtelser i forbindelse med disse behandlingsaktiviteter, nemlig med hensyn til dataminimering, opbevaringsbegrænsning, sikkerhedsforanstaltninger og behandling af klager ([40]). Som følge heraf kan enkeltpersoner stadig indgive en klage til PIPC, hvis disse principper og forpligtelser ikke overholdes, og PIPC har beføjelse til at træffe håndhævelsesforanstaltninger i tilfælde af manglende overholdelse.

([35]) Jf. navnlig artikel 18, stk. 2, og kapitel VI i PIPA.

([36]) Informationstjenester omfatter både videregivelse af oplysninger og formidlingstjenester til videregivelse af oplysninger.

([37]) Jf. artikel 2, stk. 1, nr. 3, (sammenholdt med artikel 2, stk. 1, nr. 2 og 4) i netværksloven og artikel 2, stk. 6 og 8, i telekommunikationsloven.

([38]) I det omfang koreanske udbydere af informations- og kommunikationstjenester har en direkte forbindelse til enkeltpersoner i EU (ved at tilbyde onlinetjenester), kan dette føre til direkte anvendelse af forordning (EU) 2016/679 i henhold til forordningens artikel 3, stk. 2, litra a).

([39]) I artikel 58, stk. 2, i PIPA fastsættes det endvidere, at artikel 15 og 22, artikel 27, stk. 1 og 2, artikel 34 og 37 ikke finder anvendelse på personoplysninger, der behandles ved hjælp af udstyr til visuel databehandling, der installeres og anvendes åbne steder. Da denne bestemmelse vedrører anvendelsen af videoovervågning i Korea, dvs. direkte indsamling af personoplysninger fra enkeltpersoner i Korea, er den ikke relevant i forbindelse med denne afgørelse, som omfatter overførsel af personoplysninger fra dataansvarlige/databehandlere i EU til enheder i Korea. I henhold til artikel 58, stk. 3, i PIPA finder artikel 15 (indsamling og anvendelse af personoplysninger), artikel 30 (forpligtelse til at indføre en offentlig politik for beskyttelse af privatlivets fred) og artikel 31 (forpligtelse til at udpege en databeskyttelsesansvarlig) desuden ikke anvendelse på personoplysninger, der behandles med henblik på at drive venskabsgrupper eller -foreninger (f.eks. hobbyklubber). Da sådanne grupper anses for at være af personlig karakter uden forbindelse til en erhvervsmæssig eller kommerciel aktivitet, kræves der ikke noget specifikt retsgrundlag (f.eks. samtykke fra de berørte personer) for at kunne indsamle og anvende deres oplysninger i denne sammenhæng. Alle andre bestemmelser i PIPA (f.eks. om dataminimering, formålsbegrænsning, lovlig behandling, sikkerhed og individuelle rettigheder) finder dog fortsat anvendelse. Desuden er enhver behandling af personoplysninger, der rækker ud over formålet med at oprette en social gruppe, ikke omfattet af undtagelsen.

([40]) Artikel 58, stk. 4, i PIPA indeholder mere specifikt en forpligtelse til at behandle personoplysninger i mindst muligt omfang og ikke længere end nødvendigt for at nå det tilsigtede formål og til at træffe de nødvendige foranstaltninger til sikker forvaltning og korrekt behandling af sådanne personoplysninger. Sidstnævnte omfatter tekniske, ledelsesmæssige og fysiske garantier samt foranstaltninger til at sikre en korrekt behandling af individuelle klager.

(27) For det første omfatter den delvise undtagelse personoplysninger, der indsamles i henhold til statistikloven med henblik på behandling i offentlige institutioner. Ifølge de præciseringer, der er modtaget fra den koreanske regering, vedrører personoplysninger, der behandles i denne forbindelse, normalt koreanske statsborgere og kan kun undtagelsesvis omfatte oplysninger om udlændinge, navnlig i forbindelse med statistikker om indrejse til og udrejse fra området, eller om udenlandske investeringer. Men selv i disse situationer overføres sådanne oplysninger normalt ikke fra dataansvarlige/databehandlere i Unionen, idet de som oftest indsamles direkte af de offentlige myndigheder i Korea ([41]). I lighed med, hvad der er fastsat i betragtning 162 i forordning (EU) 2016/679, er behandlingen af oplysninger i henhold til statistikloven desuden underlagt en række betingelser og garantier. Statistikloven pålægger navnlig specifikke forpligtelser, f.eks. til at sikre nøjagtighed, konsistens og upartiskhed, garantere den enkeltes ret til fortrolighed, beskytte oplysninger fra respondenter i forbindelse med statistiske forespørgsler, herunder for at forhindre, at sådanne oplysninger anvendes til andre formål end at udarbejde statistikker, og om at underlægge personalet fortrolighedskrav ([42]). Offentlige myndigheder, der behandler statistikker, skal bl.a. også overholde principperne om dataminimering, formålsbegrænsning og sikkerhed (artikel 3 og artikel 58, stk. 4, i PIPA) og give enkeltpersoner mulighed for at udøve deres rettigheder (indsigt, berigtigelse, sletning og suspension, jf. artikel 4 i PIPA). Endelig skal oplysningerne behandles i anonymiseret eller pseudonymiseret form, hvis dette gør det muligt at opfylde formålet med behandlingen (artikel 3, stk. 7, i PIPA).

(28) For det andet henviser artikel 58, stk. 1, i PIPA til personoplysninger, der indsamles eller udbedes med henblik på analyse af oplysninger vedrørende national sikkerhed. Anvendelsesområdet for og konsekvenserne af denne delvise undtagelse er nærmere beskrevet i betragtning 149.

(29) For det tredje finder den delvise undtagelse anvendelse på midlertidig behandling af personoplysninger, når dette er bydende nødvendigt af hensyn til den offentlige sikkerhed, herunder folkesundheden. Denne kategori fortolkes strengt i PIPC og er ifølge de modtagne oplysninger aldrig blevet anvendt. Den finder kun anvendelse i nødsituationer, der kræver en hurtig indsats, f.eks. for at spore smitsomme agenser eller for at redde og hjælpe ofre for naturkatastrofer ([43]). Selv i disse tilfælde omfatter den delvise undtagelse kun behandling af personoplysninger i en begrænset periode med henblik på at gennemføre en sådan foranstaltning. Situationer, hvor dette kan finde anvendelse på dataoverførsler, der er omfattet af denne afgørelse, er endnu mere begrænsede i betragtning af den ringe sandsynlighed for, at personoplysninger, der overføres fra Unionen til koreanske operatører, vil være af den type, der kan gøre den efterfølgende behandling »bydende nødvendig« i sådanne nødsituationer.

(30) Endelig finder den delvise undtagelse anvendelse på personoplysninger, der indsamles eller anvendes af pressen og i forbindelse med religiøse organisationers missionsarbejde eller politiske partiers udnævnelse af kandidater. Undtagelsen gælder kun, når personoplysninger behandles af pressen, religiøse organisationer eller politiske partier til disse specifikke formål (dvs. journalistiske aktiviteter, missionsarbejde og udnævnelse af politiske kandidater). Hvis disse enheder behandler personoplysninger til andre formål, f.eks. forvaltning af menneskelige ressourcer eller intern administration, finder PIPA fuld anvendelse.

(31) Med hensyn til pressens behandling af personoplysninger i forbindelse med journalistiske aktiviteter er balancen mellem ytringsfrihed og andre rettigheder (herunder retten til privatlivets fred) fastsat i lov om voldgift og erstatning mv. for skade forårsaget af presseartikler (presseloven) ([44]). Det fastsættes navnlig i artikel 5 i presseloven, at pressen (dvs. medieforetagender, aviser, tidsskrifter eller onlineaviser) og internetbaserede

([41]) I denne henseende pålægger artikel 33 i statistikloven offentlige institutioner at beskytte oplysninger fra respondenter i forbindelse med statistiske forespørgsler, herunder for at forhindre, at sådanne oplysninger anvendes til andre formål end at udarbejde statistikker.

([42]) Artikel 2, stk. 2-3, artikel 30, stk. 2, og artikel 33 og 34 i statistikloven.

([43]) PIPA-håndbogen, afsnittet om artikel 58.

([44]) F.eks. hedder det i artikel 4 i presseloven, at presseartikler skal være upartiske og objektive, i offentlighedens interesse, respektere den menneskelige værdighed og værdi og hverken må håne andre personer eller krænke deres rettigheder og den offentlige moral eller sociale etik.

nyhedstjenester eller multimedieforetagender ikke må krænke den enkeltes ret til privatlivets fred. Hvis der alligevel sker en krænkelse af privatlivets fred, skal den straks afhjælpes i overensstemmelse med specifikke procedurer, der er fastsat i loven. I denne henseende giver loven enkeltpersoner, der lider skade som følge af en presseartikel, en række rettigheder til at få offentliggjort en berigtigelse af falske udsagn, en berigtigelse i form af et dementi eller en ny presseartikel (hvis en presseartikel vedrører påstande om forbrydelser, som den pågældende senere frikendes for) ([45]). Enkeltpersoners krav kan afgøres direkte af medieforetagenderne (gennem en ombudsmand) ([46]), ved forlig eller voldgift (ved en specialiseret pressevoldgiftskommission) ([47]) eller ved domstolene. Enkeltpersoner kan også få erstatning, hvis de lider økonomisk tab, hvis en personlig rettighed krænkes, eller hvis de lider psykisk overlast som følge af en ulovlig handling fra pressens side (forsætlig eller uagtsom) ([48]). Pressen er fritaget for ansvar i henhold til loven, i det omfang en presseartikel, der griber ind i en persons rettigheder, ikke er i strid med sociale værdier og offentliggøres enten med den pågældende persons samtykke eller i offentlighedens interesse (og der er tilstrækkeligt grundlag for at antage, at presseartiklen stemmer overens med sandheden) ([49]).

(32) Pressens behandling af personoplysninger i forbindelse med journalistiske aktiviteter er derfor underlagt specifikke garantier i henhold til presseloven, men der er ikke de samme supplerende garantier for anvendelsen af undtagelserne i forbindelse med religiøse organisationers og politiske partiers behandlingsaktiviteter som i artikel 85, 89 og 91 i forordning (EU) 2016/679. Kommissionen finder det derfor hensigtsmæssigt at udelukke religiøse organisationer, i det omfang de behandler personoplysninger i forbindelse med deres missionsarbejde, og politiske partier, i det omfang de behandler personoplysninger i forbindelse med udnævnelsen af kandidater, fra denne afgørelses anvendelsesområde.

2.3. **Garantier, rettigheder og forpligtelser**

2.3.1. *Behandlingens lovlighed og rimelighed*

(33) Enhver behandling af personoplysninger bør være lovlig og rimelig.

(34) Dette princip er fastlagt i artikel 3, stk. 1 og 2, i PIPA og styrkes af artikel 59 i PIPA, som forbyder behandling af personoplysninger »ved brug af svig eller utilbørlige eller urimelige midler«, »uden retlig bemyndigelse« eller »uden behørig bemyndigelse« ([50]). Disse generelle principper for lovlig behandling er uddybet i artikel 15-19 i PIPA, som fastsætter de forskellige retsgrundlag for behandling (indsamling, anvendelse og videregivelse til tredjemand), herunder de omstændigheder, hvorunder dette kan indebære en ændring af formål (artikel 18 i PIPA).

([45]) Artikel 15-17 i presseloven.

([46]) Ethvert presse- eller medieforetagende skal have sin egen ombudsmand, som skal forebygge og afhjælpe eventuel skade forårsaget af pressen (f.eks. ved henstilling om offentliggørelse af en berigtigelse af presseartikler, der er falske eller skader andres omdømme), jf. artikel 6 i presseloven.

([47]) Kommissionen består af mellem 40 og 90 voldgiftsmænd udpeget af ministeren for kultur, sport og turisme blandt dommere, advokater, personer, der har beskæftiget sig med nyhedsindsamling eller -rapportering i mindst ti år, eller andre personer med ekspertise på presseområdet. Voldgiftsmænd kan ikke samtidig være offentligt ansatte, medlemmer af politiske partier eller journalister. I henhold til presselovens artikel 8 skal voldgiftsmænd udføre deres hverv uafhængigt, og de og må ikke være underlagt styring eller modtage instrukser i forbindelse med disse opgaver. Desuden er der indført særlige regler for at forebygge interessekonflikter, f.eks. ved at udelukke individuelle voldgiftsmænd fra at behandle individuelle sager, hvis deres ægtefælle eller slægtninge er part i sagen (presselovens artikel 10). Kommissionen kan behandle tvister gennem forlig eller voldgift, men kan også fremsætte henstillinger for at afhjælpe overtrædelser (presselovens artikel 5).

([48]) Presselovens artikel 30.

([49]) Presselovens artikel 5.

([50]) Artikel 59 i PIPA forbyder enhver, »som behandler eller på noget tidspunkt har behandlet personoplysninger«, at »indhente personoplysninger eller opnå samtykke til behandling af personoplysninger ved brug af svig eller utilbørlige eller urimelige midler«, at »videregive personoplysninger, der er indhentet som led i udøvelsen af erhvervsmæssig virksomhed, eller at videregive dem til tredjemand uden bemyndigelse« eller at »skade, tilintetgøre, ændre, forfalske eller videregive andres personoplysninger uden retlig bemyndigelse eller uden behørig bemyndigelse«. En overtrædelse af dette forbud kan føre til strafferetlige sanktioner, jf. artikel 71, stk. 5 og 6, og artikel 72, stk. 2, i PIPA. Artikel 70, stk. 2, i PIPA giver desuden mulighed for at pålægge en strafferetlig sanktion for at indhente personoplysninger behandlet af tredjemand ved brug af svig eller andre urimelige midler eller metoder eller for at videregive dem til tredjemand med vinding for øje eller til uretmæssige formål samt for at tilskynde til eller planlægge en sådan adfærd.

(35) I henhold til artikel 15, stk. 1, i PIPA må en dataansvarlig kun indsamle personoplysninger (inden for rammerne af formålet med indsamlingen) af et begrænset antal retlige grunde. Disse er 1) den registreredes samtykke ([51]) (nr. 1), 2) nødvendigheden af at gennemføre og opfylde en kontrakt med den registrerede (nr. 4), 3) en særlig lovbestemt tilladelse eller en nødvendighed for at opfylde en retlig forpligtelse (nr. 2), nødvendigheden ([52]) af, at en offentlig institution varetager de opgaver, der henhører under dens kompetence i henhold til lovgivningen, 4) den åbenlyse nødvendighed af at beskytte den registreredes eller tredjemands liv, legeme eller ejendom mod overhængende fare (kun hvis den registrerede ikke er i stand til at give udtryk for sin hensigt, eller hvis der ikke kan indhentes forudgående samtykke) (nr. 5), 5) nødvendigheden af at beskytte den dataansvarliges »berettigede interesse«, hvis den går »klart forud for« den registreredes interesser (og kun hvis behandlingen har en »væsentlig forbindelse« til den legitime interesse og ikke går videre, end hvad der er rimeligt) (nr. 6) ([53]). Disse grunde til behandling svarer i det væsentlige til dem, der er fastsat i artikel 6 i forordning (EU) 2016/679, herunder begrundelsen »berettiget interesse«, der svarer til begrundelsen »legitim interesse« i artikel 6, stk. 1, litra f), i forordning (EU) 2016/679.

(36) Indsamlede personoplysninger kan anvendes inden for rammerne af formålet med indsamlingen (artikel 15, stk. 1, i PIPA) eller »inden for rammer, der er rimeligt relateret « til formålet med indsamlingen, under hensyntagen til eventuelle ulemper for den registrerede, og forudsat at de nødvendige sikkerhedsforanstaltninger (f.eks. kryptering) er blevet truffet (artikel 15, stk. 3, i PIPA). For at afgøre, om formålet med anvendelsen er »rimeligt relateret« til det oprindelige indsamlingsformål, anvendes de specifikke kriterier i gennemførelsesdekretet, som svarer til kriterierne i artikel 6, stk. 4, i forordning (EU) 2016/679. Der skal navnlig være en betydelig relevans i forhold til det oprindelige formål, den videre anvendelse skal være forudsigelig (f.eks. i lyset af de omstændigheder, hvorunder oplysningerne blev indsamlet), og hvis det er muligt, skal oplysningerne pseudonymiseres ([54]). De specifikke kriterier, som den dataansvarlige anvender i forbindelse med denne vurdering, skal meddeles på forhånd i politikken for beskyttelse af privatlivets fred ([55]). Desuden er den databeskyttelsesansvarlige (jf. betragtning 94) specifikt forpligtet til at undersøge, om den videre anvendelse sker inden for disse parametre.

([51]) Samtykke skal være givet frivilligt, det skal være informeret, specifikt og givet på en af flere måder, der er fastsat ved lov. Under alle omstændigheder kan samtykke ikke indhentes ved brug af svig eller utilbørlige eller på anden måde urimelige midler (artikel 59, stk. 1, i PIPA). I henhold til artikel 4, nr. 2, i PIPA, har registrerede for det første ret til »at afgive eller nægte samtykke« og »til at definere samtykkets omfang«, og de skal informeres herom (artikel 15, stk. 2, artikel 16, stk. 2 og 3, artikel 17, stk. 2, og artikel 18, stk. 3, i PIPA). Artikel 22, stk. 5, i PIPA indeholder en supplerende garanti ved at forbyde en dataansvarlig at nægte levering af varer eller tjenesteydelser, hvis dette kan underminere den enkeltes frie valg med hensyn til at give samtykke. Dette omfatter situationer, hvor kun visse typer behandling kræver samtykke (mens andre er baseret på kontrakter), og omfatter også videre-behandling af personoplysninger indsamlet i forbindelse med levering af varer eller tjenesteydelser. For det andet skal den data-ansvarlige i henhold til artikel 15, stk. 2, artikel 17, stk. 2 og 3, og artikel 18, stk. 3, i PIPA i forbindelse med anmodningen om samtykke underrette den registrerede om de pågældende personoplysningers »særlige karakter« (f.eks. at det vedrører følsomme oplysninger, jf. artikel 17, stk. 2, nr. 2, litra a), i PIPA-gennemførelsesdekretet), om formålet med behandlingen, opbevarings-perioden og enhver modtager af oplysningerne. En sådan anmodning skal fremsættes »på en klart genkendelig måde«, hvor der skelnes mellem spørgsmål, der kræver samtykke, og andre spørgsmål (artikel 22, stk. 1-4, i PIPA). For det tredje fastsættes de specifikke metoder, hvorved den dataansvarlige skal indhente samtykke, f.eks. skriftligt samtykke med den registreredes underskrift eller samtykke ved (returnering af) e-mail, i artikel 17, stk. 1, nr. 1-6, i PIPA-gennemførelsesdekretet. PIPA giver ikke specifikt registrerede en generel ret til at trække deres samtykke tilbage, men de har ret til at få suspenderet behandlingen af oplysninger, der vedrører dem, og når denne ret udøves, indstilles behandlingen og oplysningerne slettes (jf. betragtning 78 om retten til suspen-sion).

([52]) Ifølge oplysninger fra PIPC kan offentlige institutioner kun påberåbe sig denne grund, hvis behandlingen af personoplysninger er uundgåelig, dvs. at det skal være umuligt eller urimeligt vanskeligt for institutionen at udføre sine opgaver uden at behandle oplysningerne.

([53]) Artikel 39-3 i PIPA pålægger udbydere af informations- og kommunikationstjenester specifikke (strengere) forpligtelser med hensyn til indsamling og anvendelse af personoplysninger om deres brugere. Det kræves navnlig, at udbyderen indhenter brugerens samtykke, efter at have givet oplysninger om formålet med indsamlingen/anvendelsen, de kategorier af personoplysninger, der skal indsamles, og varigheden af behandlingen af oplysningerne (artikel 39-3, stk. 1, i PIPA). Det samme gælder, når nogle af disse aspekter ændres. Manglende samtykke til indsamling af oplysninger er omfattet af strafferetlige sanktioner (artikel 71, stk. 4-5, i PIPA). Brugernes personoplysninger kan undtagelsesvis indsamles eller anvendes af udbydere af informations- og kommunikations-tjenester uden forudgående samtykke. Dette er tilfældet, 1) hvis det tydeligvis er vanskeligt at opnå samtykke på almindelig vis i forbindelse med de personoplysninger, der er nødvendige for at gennemføre kontrakten om levering af informationskommunika-tionstjenester af økonomiske og teknologiske årsager (f.eks. når der uundgåeligt frembringes personoplysninger i forbindelse med gennemførelsen af en kontrakt, f.eks. faktureringsoplysninger, adgangslogfiler og betalingsoptegnelser), 2) hvis det er nødvendigt i forbindelse med betalingen af gebyrer efter levering af informations- og kommunikationstjenester, eller 3) hvis det er tilladt i henhold til anden lovgivning (f.eks. hedder det i artikel 21, stk. 1, nr. 6, i lov om forbrugerbeskyttelse inden for elektronisk handel, at erhvervsdrivende kan indsamle personoplysninger om værger for en mindreårig for at bekræfte, om der er opnået gyldigt samtykke på vegne af den mindreårige) (artikel 39-3, stk. 2, i PIPA). Under alle omstændigheder må udbydere af informations- og kommunikationstjenester ikke nægte at levere tjenester, blot fordi brugeren ikke giver flere personoplysninger end det krævede minimum (dvs. de oplysninger, der er nødvendige for at udføre de væsentlige elementer i den pågældende tjeneste), jf. artikel 39-3, stk. 3, i PIPA.

([54]) Jf. artikel 14-2 i PIPA-gennemførelsesdekretet.

([55]) Artikel 14-2, stk. 2, i PIPA-gennemførelsesdekretet.

(37) Der gælder tilsvarende (men noget strengere) regler for videregivelse af oplysninger til tredjemand. I henhold til artikel 17, stk. 1, i PIPA kan personoplysninger videregives til tredjemand på grundlag af samtykke ([56]) eller inden for rammerne af formålet med indsamlingen, hvis oplysningerne er blevet indsamlet af en eller flere af de retlige grunde i artikel 15, stk. 1, nr. 2, 3 og 5, i PIPA. Dette udelukker navnlig enhver videregivelse baseret på den dataansvarliges »berettigede interesse«. Derudover tillader artikel 17, stk. 4, i PIPA videregivelse til tredjemand »inden for rammer, der er rimeligt relateret« til formålet med indsamlingen, under hensyntagen til eventuelle ulemper for den registrerede, og forudsat at de nødvendige sikkerhedsforanstaltninger (f.eks. kryptering) er blevet truffet. Der skal tages hensyn til de samme faktorer som i betragtning 36 for at vurdere, om videregivelsen ligger inden for rammer, der er rimeligt relateret til formålet med indsamlingen, og de samme garantier (dvs. for gennemsigtighed gennem politikken for beskyttelse af privatlivets fred og inddragelse af den databeskyttelsesansvarlige) finder anvendelse.

(38) En koreansk dataansvarligs modtagelse af personoplysninger fra Unionen betragtes som »indsamling« som omhandlet i artikel 15 i PIPA. I meddelelse nr. 2021-5 (afsnit I i bilag I til denne afgørelse) præciseres det, at det formål, hvortil oplysningerne blev overført fra den pågældende EU-enhed, er formålet med indsamlingen for den koreanske dataansvarlige. Som følge heraf er koreanske dataansvarlige, der modtager personoplysninger fra Unionen, i princippet forpligtet til at behandle sådanne oplysninger inden for rammerne af formålet med overførslen i overensstemmelse med artikel 17 i PIPA.

(39) Der gælder særlige begrænsninger, hvis den dataansvarlige ønsker at anvende personoplysningerne eller videregive dem til tredjemand til et andet formål end formålet med indsamlingen ([57]). I henhold til artikel 18, stk. 2, i PIPA kan en privat dataansvarlig undtagelsesvis ([58]) anvende personoplysninger eller videregive dem til tredjemand til et andet formål: 1) baseret på den registreredes yderligere (dvs. særskilte) samtykke, 2) hvis det er fastsat i særlige lovbestemmelser, eller 3) hvis det er åbenlyst nødvendigt for beskyttelsen af den registreredes eller tredjemands liv, legeme eller ejendom mod overhængende fare (kun hvis den registrerede ikke er i stand til at give udtryk for sin hensigt, eller hvis der ikke kan indhentes forudgående samtykke) ([59]).

(40) Offentlige institutioner kan også anvende personoplysninger eller videregive dem til tredjemand til et andet formål i visse situationer. Dette omfatter tilfælde, hvor det ellers ville være umuligt for offentlige institutioner at udføre deres lovbestemte opgaver, med forbehold af PIPC's godkendelse. Desuden kan offentlige institutioner videregive personoplysninger til en anden myndighed eller domstol, hvis dette er nødvendigt for at efterforske og retsforfølge forbrydelser eller for at rejse tiltale, for at en domstol kan udføre sine opgaver i forbindelse med verserende retssager, eller for at fuldbyrde en strafferetlig sanktion eller en kendelse om varetægtsfængsling ([60]). De kan også videregive personoplysninger til en udenlandsk regering eller international organisation for at opfylde en retlig forpligtelse i henhold til en traktat eller en international konvention, i hvilket tilfælde de også skal opfylde kravene vedrørende grænseoverskridende dataoverførsler (jf. betragtning 90).

(41) Principperne om lovlig og rimelig behandling gennemføres derfor i koreansk ret på en måde, der i det væsentlige svarer til forordning (EU) 2016/679, ved kun at tillade behandling på grundlag af legitime og klart definerede grunde. I alle nævnte tilfælde er behandlingen desuden kun tilladt, hvis det ikke er sandsynligt, at det vil »krænke den registreredes eller tredjemands interesser uretmæssigt«, hvilket kræver en afvejning af interesser. Desuden foreskriver artikel 18, stk. 5, i PIPA supplerende garantier, når den dataansvarlige videregiver personoplysninger til tredjemand, som kan omfatte et krav om at begrænse anvendelsesformålet eller -metoden eller om at indføre specifikke sikkerhedsforanstaltninger. Tredjemand er derefter forpligtet til at gennemføre de krævede foranstaltninger.

([56]) Overtrædelser af artikel 17, stk. 1, nr. 1, i PIPA kan føre til strafferetlige sanktioner (artikel 71, stk. 1, i PIPA.).

([57]) Det »tilsigtede formål« er det formål, hvortil oplysningerne blev indsamlet. Hvis oplysningerne f.eks. indsamles på grundlag af den pågældende persons samtykke, er det tilsigtede formål det formål, der meddeles den pågældende i henhold til artikel 15, stk. 2, i PIPA.

([58]) Jf. artikel 18, stk. 1, i PIPA. Overtrædelser af artikel 18, stk. 1 og 2, kan føre til strafferetlige sanktioner (artikel 71, stk. 2, i PIPA.).

([59]) Informations- og kommunikationstjenesteudbyderes anvendelse af personoplysninger eller videregivelse heraf til tredjemand til et andet formål end det oprindelige må kun finde sted af de grunde, der er anført i artikel 18, stk. 2, nr. 1 og 2, i PIPA (dvs. hvis der er indhentet yderligere samtykke, eller hvis der findes særlige bestemmelser i lovgivningen). Jf. artikel 18, stk. 2, i PIPA.

([60]) Medmindre behandlingen er nødvendig for efterforskningen af forbrydelser, tiltalerejsning og retsforfølgelse, skal offentlige institutioner, der anvender personoplysninger eller videregiver dem til tredjemand til et andet formål end formålet med indsamlingen (f. eks. hvis dette specifikt er tilladt ved lov eller er nødvendigt for at gennemføre en traktat), offentliggøre retsgrundlaget for behandlingen og formålet med og omfanget heraf på deres websted eller i statstidende og føre fortegnelser (artikel 18, stk. 4, i PIPA og artikel 15 i PIPA-gennemførelsesdekretet.).

(42) Endelig giver artikel 28-2 i PIPA mulighed for (videre)behandling af pseudonymiserede oplysninger uden den berørte persons samtykke til statistiske formål, videnskabelige forskningsformål ([61]) og arkivformål i samfundets interesse med forbehold af specifikke garantier. I lighed med forordning (EU) 2016/679 ([62]) letter PIPA derfor (videre)behandling af personoplysninger til sådanne formål inden for en ramme, der giver fornødne garantier for beskyttelse af personers rettigheder. I stedet for at anvende pseudonymisering som en mulig garanti pålægger PIPA pseudonymisering som en forudsætning for at udføre visse behandlingsaktiviteter til statistiske formål, videnskabelige forskningsformål og arkivformål i samfundets interesse (f.eks. for at kunne behandle oplysninger uden samtykke eller samkøre forskellige datasæt).

(43) Desuden indfører PIPA en række specifikke garantier, navnlig med hensyn til krævede tekniske og organisatoriske foranstaltninger, registrering, begrænsninger vedrørende dataudveksling og håndtering af mulige risici for genidentifikation. Kombinationen af de forskellige garantier, der er beskrevet i betragtning 44-48 sikrer, at behandlingen af personoplysninger i denne sammenhæng i det væsentlige er omfattet af samme beskyttelse som den, der kræves i henhold til forordning (EU) 2016/679.

(44) For det første forbyder artikel 28-5, stk. 1, i PIPA behandling af pseudonymiserede oplysninger med det formål at identificere en bestemt person. Hvis oplysninger, der kan identificere en person, alligevel frembringes under behandlingen af pseudonymiserede oplysninger, skal den dataansvarlige straks suspendere behandlingen og tilintetgøre sådanne oplysninger (artikel 28-5, stk. 2, i PIPA). Manglende overholdelse af disse bestemmelser straffes med administrative bøder og udgør en strafbar handling ([63]). Dette betyder, at selv i situationer, hvor det vil være *praktisk* muligt at genidentificere den pågældende person, er en sådan genidentifikation *retligt* forbudt.

(45) For det andet skal den dataansvarlige i forbindelse med (videre)behandling af pseudonymiserede oplysninger til sådanne formål indføre specifikke teknologiske, ledelsesmæssige og fysiske foranstaltninger for at garantere oplysningernes sikkerhed (herunder separat opbevaring og forvaltning af de oplysninger, der er nødvendige for at genoprette de pseudonymiserede oplysninger til deres oprindelige tilstand) ([64]). Desuden skal der føres fortegnelser over de pseudonymiserede oplysninger, der behandles, og over formålet med behandlingen, den tidligere anvendelse og eventuelle tredjepartsmodtagere (artikel 29-5, stk. 2, i PIPA-gennemførelsesdekretet).

(46) For det tredje indeholder PIPA endelig specifikke garantier til at forhindre, at tredjemand identificerer enkeltpersoner i forbindelse med udveksling af oplysninger. Dataansvarlige, der videregiver pseudonymiserede oplysninger til tredjemand til statistiske formål, videnskabelige forskningsformål eller arkivformål i samfundets interesse, må navnlig ikke medtage oplysninger, der kan anvendes til at identificere en bestemt person (artikel 28-2, stk. 2, i PIPA) ([65]).

(47) PIPA giver mere specifikt mulighed for at samkøre pseudonymiserede oplysninger (behandlet af forskellige dataansvarlige) til statistiske formål, videnskabelige forskningsformål eller arkivformål i samfundets interesse, men denne beføjelse gives kun til specialiserede institutioner med særlige sikkerhedsfaciliteter (artikel 28-3, stk. 1, i PIPA) ([66]). Når en dataansvarlig ansøger om samkøring af pseudonymiserede oplysninger, skal den pågældende

([61]) Videnskabelig forskning defineres i artikel 2, stk. 8, i PIPA som »forskning, der anvender videnskabelige metoder såsom teknologisk udvikling og demonstration, grundforskning, anvendt forskning og privat finansieret forskning«. Disse kategorier svarer til dem, der er fastsat i betragtning 159 i forordning (EU) 2016/679.

([62]) Se også artikel 5, stk. 1, litra b), og artikel 89, stk. 1-2, og betragtning 50 og 157 i forordning (EU) 2016/679.

([63]) Jf. artikel 28-6, stk. 1, artikel 71, stk. 4-3, og artikel 75, stk. 2, nr. 4-4, i PIPA.

([64]) Artikel 28-4 i PIPA og artikel 29-5 i PIPA-gennemførelsesdekretet. Manglende overholdelse af denne forpligtelse er underlagt administrative og strafferetlige sanktioner, jf. artikel 73, stk. 1, og artikel 75, stk. 2, nr. 6, i PIPA.

([65]) Overtrædelser af disse krav kan føre til strafferetlige sanktioner (artikel 71, stk. 2, i PIPA.). PIPC begyndte straks at håndhæve disse nye regler, f.eks. i sin afgørelse af 28. april 2021, hvor den pålagde en virksomhed, der blandt andre overtrædelser af PIPA ikke opfyldte kravet i artikel 28-2, stk. 2, i PIPA, en bøde og korrigerende foranstaltninger, se https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([66]) For at blive udpeget som en sådan specialiseret institution (et »datasamkøringsekspertbureau«) skal der indgives en ansøgning til PIPC sammen med dokumentation, herunder med nærmere oplysninger om de faciliteter og det udstyr, der er indført for sikker samkøring af pseudonymiserede oplysninger, og som påviser, at ansøgeren beskæftiger mindst tre fuldtidsansatte med kvalifikationer eller erfaring inden for beskyttelse af personoplysninger (artikel 29-2, stk. 1-2, i PIPA-gennemførelsesdekretet). Detaljerede krav, f.eks. vedrørende personalets kvalifikationer, tilgængelige faciliteter, sikkerhedsforanstaltninger, interne politikker og procedurer samt finansielle krav, er fastsat i PIPC-meddelelse nr. 2020-9 om samkøring og frigivelse af pseudonymiserede oplysninger (skema I). En udpegelse som datasamkøringsekspertbureau kan tilbagekaldes af PIPC (efter afholdelse af en høring) af visse grunde, f.eks. hvis bureauet ikke længere opfylder de sikkerhedsstandarder, der kræves for udpegelsen, eller hvis der er opstået et brud på datasikkerheden i forbindelse med en samkøring af data (artikel 29-2, stk. 5-6, i PIPA-gennemførelsesdekretet). PIPC skal offentliggøre hver udpegelse (eller tilbagekaldelse af udpegelse) af et datasamkøringsekspertbureau (artikel 29-2, stk. 7, i PIPA-gennemførelsesdekretet).

indsende dokumentation, herunder om de oplysninger, der skal samkøres, om formålet med samkøringen samt om de foreslåede sikkerhedsforanstaltninger til behandling af de samkørte oplysninger ([67]). For at muliggøre denne samkøring skal den dataansvarlige sende de oplysninger, der skal samkøres, til den specialiserede institution og levere en »samkøringsnøgle« (dvs. de oplysninger, der er blevet anvendt til pseudonymisering) til Koreas internet- og sikkerhedsagentur ([68]). Agenturet genererer »samkøringsnøglelinkdata« (som gør det muligt at forbinde forskellige ansøgeres samkøringsnøgler med henblik på at samkøre datasættene) og videregiver dem til den specialiserede institution ([69]).

(48) Den dataansvarlige, der har anmodet om en samkøring, kan analysere de samkørte oplysninger hos den specialiserede institution i et rum, hvor der er indført specifikke tekniske, fysiske og administrative sikkerhedsforanstaltninger (artikel 29-3 i PIPA-gennemførelsesdekretet). Dataansvarlige, der bidrager med et datasæt til en sådan samkøring, må kun eksportere de samkørte data fra den specialiserede institution efter yderligere pseudonymisering eller anonymisering af de samkørte data og med den pågældende institutions godkendelse (artikel 28-3, stk. 2, i PIPA) ([70]). Når det overvejes, om der skal gives en sådan godkendelse, vurderer institutionen forbindelsen mellem de samkørte data og formålet med behandlingen, og om der er udarbejdet en særlig sikkerhedsplan for anvendelsen af sådanne data ([71]). Det er ikke tilladt at eksportere de samkørte oplysninger fra institutionen, hvis oplysningerne indeholder data, der gør det muligt at identificere en person ([72]). Endelig overvåges den specialiserede institutions samkøring og frigivelse af pseudonymiserede oplysninger af PIPC (artikel 29-4, stk. 3, i PIPA-gennemførelsesdekretet).

2.3.2. *Behandling af særlige kategorier af personoplysninger*

(49) Der bør være specifikke garantier, når »særlige kategorier« af oplysninger behandles.

(50) PIPA indeholder specifikke regler for behandling af følsomme oplysninger ([73]), der defineres som personoplysninger om ideologi, tro, optagelse i eller udtræden af en fagforening eller et politisk parti, en persons politiske holdninger, sundhed og seksualitet samt andre personoplysninger, der kan true den registreredes ret til privatlivets fred »mærkbart«, og som er identificeret som følsomme oplysninger ved præsidentielt dekret ([74]). Ifølge præciseringerne fra PIPC fortolkes seksuallivet således, at det også omfatter den enkeltes seksuelle orientering eller præferencer ([75]). Endvidere tilføjer artikel 18 i gennemførelsesdekretet yderligere kategorier til gruppen af følsomme oplysninger, navnlig DNA-oplysninger fra genetiske test og oplysninger om straffedomme. Den nylige ændring af PIPA-gennemførelsesdekretet har yderligere udvidet begrebet følsomme oplysninger ved at medtage personoplysninger om race eller etnisk oprindelse og biometriske oplysninger ([76]). Efter denne ændring svarer begrebet følsomme oplysninger i PIPA i det væsentlige til begrebet i artikel 9 i forordning (EU) 2016/679.

(51) I henhold til artikel 23, stk. 1, i PIPA og i lighed med bestemmelsen i artikel 9, stk. 1, i forordning (EU) 2016/679 er behandling af følsomme oplysninger generelt forbudt, medmindre en af de nævnte undtagelser finder anvendelse ([77]). Disse begrænser behandlingen til tilfælde, hvor den dataansvarlige underretter den registrerede i

([67]) Artikel 8, stk. 1-2, i meddelelse nr. 2020-9 om samkøring og frigivelse af pseudonymiserede oplysninger.
([68]) Artikel 2, stk. 3 og 6, og artikel 9, stk. 1, i meddelelse nr. 2020-9 om samkøring og frigivelse af pseudonymiserede oplysninger.
([69]) Artikel 2, stk. 4, og artikel 9, stk. 2-3, i meddelelse nr. 2020-9 om samkøring og frigivelse af pseudonymiserede oplysninger. Den specialiserede institution skal straks tilintetgøre samkøringsnøglelinkdataene efter en samkøring (artikel 9, stk. 4, i meddelelsen).
([70]) Overtrædelser af kravene vedrørende samkøring af datasæt kan føre til pålæggelse af strafferetlige sanktioner (artikel 71, stk. 4-2, i PIPA). Se også artikel 29-2, stk. 4, i PIPA-gennemførelsesdekretet.
([71]) Proceduren for godkendelse af frigivelse af samkørte data er fastsat i artikel 11 i meddelelse nr. 2020-9 om samkøring og frigivelse af pseudonymiserede oplysninger. Den specialiserede institution skal navnlig nedsætte et »frigivelsesudvalg« bestående af medlemmer med et indgående kendskab til og erfaring med databeskyttelse.
([72]) Artikel 29-2, stk. 4, i PIPA-gennemførelsesdekretet, og meddelelse nr. 2020-9, artikel 11.
([73]) Behovet for at yde specifik beskyttelse i forbindelse med behandling af følsomme oplysninger såsom oplysninger om sundhed eller seksuel adfærd er også blevet anerkendt af den koreanske forfatningsdomstol, jf. forfatningsdomstolens afgørelse HunMa 1139 af 31. maj 2007.
([74]) Artikel 23, stk. 1, i PIPA.
([75]) Se også PIPA-håndbogen, kapitel XII, afsnit 2 om artikel 23 (s. 157-164).
([76]) Personoplysninger, der følger af en specifik teknisk behandling af oplysninger om en persons fysiske, fysiologiske eller adfærdsmæssige karakteristika med henblik på en entydig identifikation af vedkommende.
([77]) Manglende overholdelse af disse krav kan føre til sanktioner i henhold til artikel 71, nr. 3, i PIPA.

overensstemmelse med artikel 15 og 17 i PIPA og indhenter særskilt samtykke (dvs. adskilt fra samtykke til behandling af andre personoplysninger), eller hvor behandlingen er påkrævet eller tilladt i henhold til loven. Offentlige myndigheder kan også behandle biometriske oplysninger, DNA-oplysninger indhentet ved gentestning, personoplysninger om race eller etnisk oprindelse og oplysninger om straffedomme, på grundlag, som udelukkende kan påberåbes af dem (f.eks. hvis det er nødvendigt for efterforskningen af forbrydelser, eller hvis det er nødvendigt for, at en domstol kan komme videre med en sag) ([78]). Retsgrundlaget for behandling af følsomme oplysninger er mere begrænset end for andre typer personoplysninger, og det er endnu mere restriktivt i koreansk ret end i artikel 9, stk. 2, i forordning (EU) 2016/679.

(52) Desuden understreges det i artikel 23, stk. 2, i PIPA — manglende overholdelse, der kan føre til sanktioner ([79]) — at det er særlig vigtigt at sikre en tilstrækkelig sikker behandling af følsomme oplysninger, således at de »ikke går tabt, stjæles, videregives, forfalskes, ændres eller beskadiges.« Selv om dette er et generelt krav i henhold til artikel 29 i PIPA, gør artikel 3, stk. 4, det klart, at sikkerhedsniveauet skal tilpasses den type personoplysninger, der behandles, hvilket betyder, at der skal tages hensyn til de særlige risici, der er forbundet med behandlingen af følsomme oplysninger. Desuden skal databehandlingen altid foretages »på en måde, der minimerer risikoen for at krænke« den registreredes ret til privatlivets fred og om muligt »anonymt« (artikel 3, stk. 6 og 7, i PIPA). Disse krav er særlig relevante, når behandlingen vedrører følsomme oplysninger.

2.3.3. *Formålsbegrænsning*

(53) Personoplysninger skal indsamles til et specifikt formål og må ikke behandles på en måde, der er uforenelig med behandlingsformålet.

(54) Dette princip sikres ved artikel 3, stk. 1, og 2, i PIPA, hvori det fastsættes, at den dataansvarlige »specificerer og udtrykkeligt angiver« formålet med behandlingen, behandler personoplysninger på en hensigtsmæssig måde, der er nødvendig til dette formål, og må ikke anvende dem til andre formål. Det generelle princip om formålsbegrænsning bekræftes også i artikel 15, stk. 1, artikel 18, stk. 1, og artikel 19 og — for databehandlere (såkaldte »outsourcingpartnere«) — i artikel 26, stk. 1, nr. 1, og stk. 5 og 7, i PIPA). Personoplysninger må i princippet navnlig kun anvendes og videregives til tredjemand inden for rammerne af det formål, hvortil de blev indsamlet (artikel 15, stk. 1, og artikel 17, stk. 1, nr. 2). Behandling til et foreneligt formål, dvs. »inden for rammer, der er rimeligt relateret til det oprindelige formål med indsamlingen«, må kun finde sted, hvis den ikke påvirker de berørte registrerede negativt, og hvis der træffes de nødvendige sikkerhedsforanstaltninger (f.eks. kryptering) (artikel 15, stk. 3, og artikel 17, stk. 4, i PIPA). For at afgøre, om viderebehandlingen er til et foreneligt formål, indeholder PIPA-gennemførelsesdekretet en liste over specifikke kriterier, der svarer til dem, der er fastsat i artikel 6, stk. 4, i forordning (EU) 2016/679, jf. betragtning 36.

(55) Som forklaret i betragtning 38 er formålet med indsamlingen, når koreanske dataansvarlige modtager personoplysninger fra Unionen, det formål, hvortil oplysningerne overføres. Den dataansvarlige kan kun undtagelsesvis ændre formålet i specifikke (opregnede) tilfælde (artikel 18, stk. 2, nr. l-3, i PIPA, se også betragtning 39). I det omfang en ændring af formålet er tilladt ved lov, skal den grundlæggende ret til privatlivets fred og databeskyttelse samt de principper om nødvendighed og proportionalitet, der er fastsat i den koreanske forfatning, respekteres i denne lovgivning. Desuden indeholder artikel 18, stk. 2, og 5, i PIPA supplerende garantier, navnlig kravet om, at en sådan ændring af formål ikke må krænke den registreredes interesser uretmæssigt, hvilket altid kræver en afvejning af interesser. Dette sikrer et beskyttelsesniveau, der i det væsentlige svarer til niveauet i henhold til artikel 5, stk. 1, litra b), og artikel 6 sammenholdt med betragtning 50 i forordning (EU) 2016/679.

2.3.4. *Oplysningernes rigtighed og minimering*

(56) Personoplysninger skal være korrekte og om nødvendigt ajourførte. Oplysningerne skal også være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles.

([78]) I henhold til artikel 18 i PIPA-gennemførelsesdekretet er de deri anførte kategorier af oplysninger udelukket fra bestemmelsen i lovens artikel 23, stk. 1, når de behandles af en offentlig institution i henhold til artikel 18, stk. 2, nr. 5-9, i PIPA.

([79]) Jf. artikel 73, nr. 1, og artikel 75, stk. 2, nr. 6, i PIPA.

(57) Princippet om rigtighed anerkendes ligeledes i artikel 3, stk. 3, i PIPA, som kræver, at personoplysninger er »korrekte, fuldstændige og ajourførte i det omfang, det er nødvendigt i forhold til de formål«, hvortil oplysningerne behandles. Dataminimering er påkrævet i henhold til artikel 3, stk. 1 og 6, og artikel 16, stk. 1, i PIPA, hvori det fastsættes, at den dataansvarlige (kun) indsamler personoplysninger »i mindst muligt omfang« for at nå det tilsigtede formål, og at den dataansvarlige bærer bevisbyrden i denne henseende. Hvis det er muligt at opfylde formålet med indsamlingen ved at behandle oplysninger i anonymiseret form, bør de dataansvarlige bestræbe sig på at gøre dette (artikel 3, stk. 7, i PIPA).

2.3.5. *Opbevaringsbegrænsning*

(58) Personoplysninger bør i princippet ikke opbevares længere end nødvendigt til de formål, hvortil personoplysningerne behandles.

(59) Princippet om opbevaringsbegrænsning er ligeledes fastsat i artikel 21, stk. 1, i PIPA ([80]), som pålægger den dataansvarlige straks at »tilintetgøre« ([81]) personoplysninger, når formålet med behandlingen er opfyldt, eller når opbevaringsperioden er udløbet (alt efter hvad der indtræffer først), medmindre yderligere opbevaring er påkrævet i henhold til loven ([82]). I sidstnævnte tilfælde »opbevares og forvaltes de pågældende personoplysninger adskilt fra andre personoplysninger« (artikel 21, stk. 3, i PIPA).

(60) Artikel 21, stk. 1, i PIPA finder ikke anvendelse, når pseudonymiserede oplysninger behandles til statistiske formål, videnskabelige forskningsformål eller arkivformål i samfundets interesse ([83]). For ligeledes at sikre princippet om opbevaringsbegrænsning i dette tilfælde pålægger meddelelse nr. 2021-5 dataansvarlige at anonymisere oplysningerne i overensstemmelse med artikel 58-2 i PIPA, hvis oplysningerne ikke er blevet tilintetgjort, når det specifikke formål med behandlingen er opfyldt ([84]).

2.3.6. *Datasikkerhed*

(61) Personoplysninger bør behandles på en måde, der garanterer deres sikkerhed, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse. Med henblik herpå bør de erhvervsdrivende træffe passende tekniske eller organisatoriske foranstaltninger for at beskytte personoplysninger mod mulige trusler. Disse foranstaltninger bør vurderes under hensyntagen til det aktuelle tekniske niveau, de dermed forbundne omkostninger og behandlingens karakter, omfang, sammenhæng og formål samt risiciene for den enkeltes rettigheder.

(62) Et lignende sikkerhedsprincip er fastsat i artikel 3, stk. 4, i PIPA, der pålægger dataansvarlige at behandle »personoplysninger sikkert i overensstemmelse med behandlingsmetoder, typer mv. af personoplysninger under hensyntagen til risikoen for krænkelse af den registreredes rettigheder og alvoren af de pågældende risici«. Desuden behandler den dataansvarlige »personoplysninger på en måde, der minimerer risikoen for at krænke den registreredes ret til privatlivets fred«, og bestræber sig i denne forbindelse på at behandle personoplysninger anonymt eller i pseudonymiseret form, hvis det er muligt (artikel 3, stk. 6 og 7, i PIPA).

(63) Disse generelle krav uddybes yderligere i artikel 29 i PIPA, ifølge hvilken enhver dataansvarlig »træffer de tekniske, ledelsesmæssige og fysiske foranstaltninger, f.eks. udarbejdelse af en intern forvaltningsplan og opbevaring af loginregistreringer mv., der er nødvendige for at garantere sikkerheden i henhold til præsidentielt dekret, således

([80]) Artikel 8 (sammenholdt med artikel 8-2 i gennemførelsesdekretet, artikel 11 (sammenholdt med artikel 12, stk. 2, i gennemførelsesdekretet).

([81]) Om metoderne til tilintetgørelse af personoplysninger henvises til artikel 16 i PIPA-gennemførelsesdekretet. I artikel 21, stk. 2, i PIPA præciseres det, at dette skal omfatte »nødvendige foranstaltninger til at forhindre genoprettelse«.

([82]) Manglende overholdelse af dette krav kan føre til strafferetlige sanktioner i (artikel 73, stk. 1 og 2, i PIPA). Artikel 39-6 PIPA pålægger udbydere af informations- og kommunikationstjenester et yderligere krav om at slette personoplysninger om brugere, der ikke har gjort brug af de tilbudte informations- og kommunikationstjenester i mindst et år (medmindre yderligere opbevaring er påkrævet ved lov eller efter anmodning fra brugeren). Personer skal informeres om den påtænkte sletning af deres oplysninger 30 dage før udløbet af fristen på et år (artikel 39-6, stk. 2, i PIPA og artikel 48-5, stk. 3, i PIPA-gennemførelsesdekretet). Hvis loven kræver yderligere opbevaring, skal de opbevarede oplysninger opbevares adskilt fra andre brugeroplysninger og må kun anvendes eller videregives i overensstemmelse med den pågældende lov (artikel 48-5, stk. 1-2, i PIPA-gennemførelsesdekretet).

([83]) Artikel 28-7 i PIPA.

([84]) Meddelelse nr. 2021-5 (bilag I), afsnit 4.

at personoplysningerne ikke går tabt, stjæles, videregives, forfalskes, ændres eller beskadiges.« Disse foranstaltninger præciseres i artikel 30, stk. 1, i PIPA-gennemførelsesdekretet, hvor der henvises til 1) udarbejdelse og gennemførelse af en intern forvaltningsplan for sikker behandling af personoplysninger, 2) adgangskontrol og -begrænsninger, 3) indførelse af krypteringsteknologi til sikker opbevaring og videregivelse af personoplysninger, 4) loginregistreringer, 5) sikkerhedsprogrammer og 6) fysiske foranstaltninger såsom et sikkert opbevarings- eller låsningssystem ([85]).

(64) Desuden gælder der særlige forpligtelser i tilfælde af brud på datasikkerheden (artikel 34 i PIPA sammenholdt med artikel 39 og 40 i PIPA-gennemførelsesdekretet) ([86]). Den dataansvarlige skal navnlig straks give de berørte registrerede nærmere oplysninger om bruddet ([87]), herunder oplysninger om (obligatoriske) modforanstaltninger truffet af den dataansvarlige og om, hvad de registrerede kan gøre for at minimere risikoen for skade (artikel 34, stk. 1 og 2, i PIPA) ([88]). Hvis bruddet på datasikkerheden berører mindst 1 000 registrerede, indberetter den dataansvarlige straks også bruddet på datasikkerheden og de modforanstaltninger, der er truffet, til PIPC og Koreas internet- og sikkerhedsagentur, som kan yde teknisk bistand (artikel 34, stk. 3, i PIPA sammenholdt med artikel 39 i PIPA-gennemførelsesdekretet). Dataansvarlige er ansvarlige for skade som følge af brud på datasikkerheden i henhold til bestemmelserne i civilloven om ansvar uden for kontraktforhold (se også afsnit 2.5 om prøvelsesadgang) ([89]).

(65) Den dataansvarlige skal i forbindelse med opfyldelsen af sine sikkerhedsforpligtelser bistås af en databeskyttelsesansvarlig, hvis opgaver bl.a. omfatter opbygning af et internt kontrolsystem »for at forhindre videregivelse, misbrug og forkert anvendelse af personoplysninger« (artikel 31, stk. 2, nr. 4, i PIPA). Desuden har den dataansvarlige pligt til at føre »passende kontrol og tilsyn« med medarbejdere, der behandler personoplysninger, herunder med hensyn til sikker forvaltning heraf. Dette omfatter den nødvendige uddannelse af medarbejdere (artikel 28, stk. 1 og 2, i PIPA). Endelig skal den dataansvarlige i tilfælde af outsourcet behandling stille krav til »outsourcingpartneren«, bl.a. vedrørende sikker forvaltning af personoplysninger (»tekniske og ledelsesmæssige garantier«), og den dataansvarlige skal føre tilsyn med, hvordan disse gennemføres gennem inspektioner (artikel 26, stk. 1 og 4, i PIPA sammenholdt med artikel 28, stk. 1, nr. 3, 4 og 6, i PIPA-gennemførelsesdekretet).

2.3.7. *Gennemsigtighed*

(66) De registrerede skal informeres om de vigtigste elementer i behandlingen af deres personoplysninger.

([85]) Med hensyn til informations- og kommunikationstjenesteudbyderes behandling af personoplysninger fastsættes det udtrykkeligt i artikel 39-5 i PIPA, at antallet af personer, der håndterer brugernes personoplysninger, skal begrænses til et minimum. Desuden sikrer udbydere af informations- og kommunikationstjenester, at brugernes personoplysninger ikke eksponeres for offentligheden via informations- og kommunikationsnetværket (artikel 39-10, stk. 1, i PIPA). Eksponerede oplysninger skal slettes eller blokeres efter anmodning fra PIPC (artikel 39-10, stk. 2, i PIPA). Mere generelt er udbydere af informations- og kommunikationstjenester (og tredjemænd, der modtager brugernes personoplysninger) underlagt yderligere sikkerhedsforpligtelser, jf. artikel 48-2 i PIPA-gennemførelsesdekretet, f.eks. vedrørende udarbejdelse og gennemførelse af en intern forvaltningsplan for sikkerhedsforanstaltninger, foranstaltninger til at sikre adgangskontrol, kryptering, brug af software til at afsløre ondsindede programmer mv.

([86]) Der er desuden et generelt forbud mod at skade, tilintetgøre, ændre, forfalske eller lække personoplysninger uden retlig bemyndigelse, jf. artikel 59, nr. 3, i PIPA.

([87]) Kravet om at underrette den berørte person finder ikke anvendelse ved brud på datasikkerheden i forbindelse med pseudonymiserede oplysninger, der behandles til statistiske formål, videnskabelige forskningsformål eller arkivformål i samfundets interesse (artikel 28-7 i PIPA, som indeholder en undtagelse fra artikel 34, stk. 1, og artikel 39-4 i PIPA). Sikring af individuel underretning ville kræve, at den berørte dataansvarlige skulle identificere personer ud fra det pseudonymiserede datasæt, hvilket er udtrykkeligt forbudt i henhold til artikel 28-5 i PIPA. Det generelle krav om anmeldelse af brud på datasikkerheden (til PIPC) gælder dog fortsat.

([88]) Anmeldelseskravene, herunder tidsfristerne herfor og muligheden for en anmeldelse »i etaper«, præciseres yderligere i artikel 40 i PIPA-gennemførelsesdekretet. Der gælder strengere regler for udbydere af informations- og kommunikationstjenester, som skal underrette den registrerede og PIPC senest 24 timer efter, at de er blevet klar over, at personoplysningerne er gået tabt, stjålet eller lækket (artikel 39-4, stk. 1, i PIPA). Denne underretning skal indeholde nærmere oplysninger om de personoplysninger, der er blevet lækket, hvornår dette skete, de foranstaltninger, som brugeren kan træffe, de modforanstaltninger, som udbyderen har truffet, og kontaktoplysningerne for den afdeling, som brugeren kan henvende sig til (artikel 39-4, stk. 1, nr. 1-5, i PIPA). Hvis der er en rimelig grund til f.eks. ikke at have brugerens kontaktoplysninger, kan der anvendes andre meddelelsesmetoder, f.eks. ved at gøre oplysningerne offentligt tilgængelige på et websted (artikel 39-4, stk. 1, i PIPA sammenholdt med artikel 48-4, stk. 4 ff., i PIPA-gennemførelsesdekretet). I så fald skal PIPC underrettes om årsagerne (artikel 34-4, stk. 3, i PIPA).

([89]) Jf. f.eks. højesterets afgørelser 2011Da59834, 2011Da59858 og 2011Da59841 af 26. december 2012. Et resumé på engelsk findes her: http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm.

(67) Dette sikres på forskellige måder i det koreanske system. Bortset fra retten til information i henhold til artikel 4, nr. 1, (generelt) og artikel 20, stk. 1, i PIPA (for personoplysninger indsamlet fra tredjemand) samt retten til indsigt i henhold til artikel 35 i PIPA indeholder PIPA et generelt krav om gennemsigtighed med hensyn til formålet med behandlingen (artikel 3, stk. 1, i PIPA) og specifikke gennemsigtighedskrav, hvis behandlingen er baseret på samtykke (artikel 15, stk. 2, artikel 17, stk. 2, og artikel 18, stk. 3, i PIPA) ([90]). Desuden pålægger artikel 20, stk. 2, i PIPA visse dataansvarlige — for hvem behandlingen overstiger visse tærskler ([91]) — at underrette den registrerede, hvis personoplysninger de har modtaget fra tredjemand, om oplysningskilden, formålet med behandlingen og den registreredes ret til at kræve, at behandlingen suspenderes, medmindre en sådan underretning viser sig umulig på grund af manglende kontaktoplysninger. Der gælder undtagelser for visse persondatafiler, der opbevares af offentlige myndigheder, navnlig filer med oplysninger, der behandles til nationale sikkerhedsformål eller med henblik på andre særlig vigtige (»alvorlige«) nationale interesser eller strafferetlig håndhævelse, eller hvis underretningen sandsynligvis vil skade en anden persons liv eller legeme eller uretmæssigt skader en anden persons ejendom og andre interesser, dog kun hvis de pågældende offentlige eller private interesser går »klart forud for« de berørte registreredes rettigheder (artikel 20, stk. 4, i PIPA). Dette kræver en afvejning af interesser.

(68) Desuden pålægger artikel 3, stk. 5, i PIPA dataansvarlige at offentliggøre deres politik for beskyttelse af privatlivets fred (og andre spørgsmål vedrørende behandling af personoplysninger). Dette krav præciseres yderligere i artikel 30 i PIPA sammenholdt med artikel 31 i PIPA-gennemførelsesdekretet. I henhold til disse bestemmelser skal den offentlige politik for beskyttelse af privatlivets fred bl.a. indeholde oplysninger om 1) de typer personoplysninger, der behandles, 2) formålet med behandlingen, 3) opbevaringsperioden, 4) hvorvidt personoplysninger videregives til tredjemand ([92]), 5) enhver form for outsourcet behandling, 6) den registreredes rettigheder og om, hvordan de skal udøves, og 7) kontaktoplysninger (herunder navnet på den databeskyttelsesansvarlige eller den interne afdeling, der er ansvarlig for at sikre overholdelsen af databeskyttelsesreglerne og klagebehandling). Politikken for beskyttelse af privatlivets fred skal offentliggøres på en sådan måde, at de registrerede »let kan genkende den« (artikel 30, stk. 2, i PIPA) ([93]), og løbende ajourføres (artikel 31, stk. 2, i PIPA-gennemførelsesdekretet).

(69) Offentlige institutioner er navnlig underlagt en yderligere forpligtelse til at registrere følgende oplysninger hos PIPC: 1) navnet på den offentlige institution, 2) grundene til og formålene med behandlingen af persondatafilerne, 3) nærmere oplysninger om de registrerede personoplysninger, 4) behandlingsmetoden, 5) opbevaringsperioden, 6) antallet af registrerede, hvis personoplysninger opbevares, 7) den afdeling, der behandler de registreredes anmodninger, og 8) modtagerne af personoplysninger, hvis oplysningerne videregives rutinemæssigt eller gentagne gange (artikel 32, stk. 1, i PIPA) ([94]). Registrerede persondatafiler offentliggøres af PIPC, og offentlige institutioner skal også angive dette i deres politik for beskyttelse af privatlivets fred (artikel 30, stk. 1, og artikel 32, stk. 4, i PIPA).

(70) For at øge gennemsigtigheden for registrerede i Unionen, hvis personoplysninger overføres til Korea på grundlag af denne afgørelse, pålægger afsnit 3, nr. i) og nr. ii), i meddelelse nr. 2021-5 (bilag I) yderligere gennemsigtighedskrav. For det første skal koreanske dataansvarlige, der modtager personoplysninger fra Unionen på grundlag af denne afgørelse, uden unødig forsinkelse (og under alle omstændigheder senest en måned efter overførslen) underrette de berørte registrerede om navn og kontaktoplysninger på de enheder, der overfører og

([90]) Når personoplysninger behandles med den berørte persons samtykke, skal den dataansvarlige navnlig oplyse den pågældende om formålet med behandlingen, præcisere de oplysninger, der skal behandles, og oplyse om modtageren af oplysningerne, varigheden af den periode, hvori personoplysningerne opbevares og anvendes, samt om den pågældendes ret til at nægte samtykke (og enhver ulempe som følge heraf).

([91]) I henhold til artikel 15-2, stk. 1, i PIPA-gennemførelsesdekretet vedrører dette dataansvarlige, der behandler følsomme oplysninger om mindst 50 000 registrerede, eller »normale« personoplysninger om mindst 1 mio. registrerede. I artikel 15-2, stk. 2, i PIPA-gennemførelsesdekretet fastsættes metoderne og fristerne for underretningen og i artikel 15-2, stk. 3, kravet om at føre visse fortegnelser herover. Desuden gælder der særlige regler for visse kategorier af udbydere af informations- og kommunikationstjenester (udbydere med salgsindtægter på mindst 10 mia. WON det foregående år, eller udbydere, der har opbevaret/forvaltet personoplysninger om mindst en million brugere om dagen i gennemsnit i de tre måneder, der går forud for udgangen af det foregående år), som er forpligtet til regelmæssigt at underrette brugerne om anvendelsen af deres personoplysninger, medmindre dette viser sig umuligt på grund af manglende kontaktoplysninger (artikel 39-8 i PIPA og artikel 48-6 i PIPA-gennemførelsesdekretet).

([92]) Ifølge de oplysninger, der er modtaget fra den koreanske regering, indebærer dette en forpligtelse til at angive modtageren eller modtagerne individuelt i den offentlige politik for beskyttelse af privatlivets fred.

([93]) Der er fastsat yderligere bestemmelser i artikel 31, stk. 3, i PIPA-gennemførelsesdekretet.

([94]) Registreringskravet gælder ikke for visse typer persondatafiler, f.eks. filer vedrørende nationale sikkerhedsspørgsmål, diplomatiske hemmeligheder, strafferetlige efterforskninger, retsforfølgelse, straf, efterforskning af skattekriminalitet, eller filer, der udelukkende vedrører interne arbejdspræstationer (artikel 32, stk. 2, i PIPA).

modtager oplysningerne, om de overførte personoplysninger (eller kategorier af personoplysninger), formålet med den koreanske dataansvarliges indsamling, opbevaringsperioden og rettighederne i henhold til PIPA. For det andet skal de registrerede, når personoplysninger modtaget fra Unionen på grundlag af denne afgørelse videregives til tredjemand, bl.a. underrettes om modtageren, de personoplysninger eller kategorier af personoplysninger, der skal videregives, det land, som oplysningerne videregives til (hvis det er relevant), samt om rettighederne i henhold til PIPA ([95]). På denne måde sikrer meddelelsen, at enkeltpersoner i EU fortsat informeres om de specifikke dataansvarlige, der behandler deres oplysninger, og at de kan udøve deres rettigheder over for de relevante enheder.

(71) Afsnit 3, nr. iii), i meddelelsen (bilag I) tillader visse begrænsede og kvalificerede undtagelser fra disse yderligere gennemsigtighedsforpligtelser, der i det væsentlige svarer til dem, der er fastsat i forordning (EU) 2016/679. Underretning af registrerede i Unionen er navnlig ikke påkrævet, 1) hvis og så længe det er nødvendigt at begrænse underretningen af hensyn til visse samfundsinteresser (f.eks. hvis oplysningerne behandles til nationale sikkerhedsformål eller i forbindelse med igangværende strafferetlige efterforskninger), i det omfang disse mål i samfundets interesse går klart forud for den registreredes rettigheder, 2) hvis den registrerede allerede er bekendt med oplysningerne, 3) hvis og så længe underretningen sandsynligvis vil skade den registreredes eller en anden persons liv eller legeme eller uretmæssigt krænke en anden persons ejendomsinteresser, hvis disse rettigheder eller interesser går klart forud for den registreredes rettigheder, eller 4) hvis der ikke findes kontaktoplysninger for de pågældende personer, eller hvis der kræves en uforholdsmæssig stor indsats for at underrette dem. Ved afgørelsen af, om det er muligt at kontakte den registrerede, eller om dette indebærer en uforholdsmæssig stor indsats, tages der hensyn til muligheden for at samarbejde med dataeksportøren i Unionen.

(72) Reglerne i betragtning 67-71 sikrer derfor et beskyttelsesniveau med hensyn til gennemsigtighed, som i det væsentlige svarer til det niveau, der er fastsat i forordning (EU) 2016/679.

2.3.8. *Individuelle rettigheder*

(73) Registrerede bør have visse rettigheder, som kan gøres gældende over for den dataansvarlige eller databehandleren, navnlig retten til indsigt i oplysninger, retten til berigtigelse, retten til at gøre indsigelse mod behandlingen og retten til at få oplysninger slettet. Samtidig kan sådanne rettigheder være underlagt begrænsninger, for så vidt som disse begrænsninger er nødvendige og forholdsmæssige for at beskytte vigtige mål af almen interesse.

(74) I henhold til artikel 3, stk. 5, i PIPA garanterer den dataansvarlige de registreredes rettigheder, der er anført i artikel 4 i PIPA og yderligere præciseret i artikel 35-37, 39 og 39-2 i PIPA.

(75) For det første har enkeltpersoner ret til oplysning og indsigt. Når den dataansvarlige har indsamlet personoplysninger fra tredjemand — hvilket altid vil være tilfældet, når oplysningerne overføres fra Unionen — har registrerede generelt ret til at modtage oplysninger om 1) »kilden« til de indsamlede personoplysninger (dvs. overdrageren), 2) formålet med behandlingen og 3) den registreredes ret til at kræve, at behandlingen suspenderes (artikel 20, stk. 1, i PIPA). Der gælder begrænsede undtagelser, nemlig når en sådan underretning sandsynligvis vil skade en anden persons liv eller legeme eller »uretmæssigt skader en anden persons ejendom og andre interesser«, dog kun hvis disse tredjemandsinteresser går »klart forud for« den registreredes rettigheder (artikel 20, stk. 4, nr. 2, i PIPA).

(76) Desuden giver artikel 35, stk. 1 og 3, i PIPA sammenholdt med artikel 41, stk. 4, i PIPA-gennemførelsesdekretet de registrerede ret til indsigt i deres personoplysninger ([96]). Retten til indsigt omfatter bekræftelse af behandlingen, oplysninger om typen af behandlede oplysninger, formålet med behandlingen, opbevaringsperioden samt enhver videregivelse til tredjemand og udlevering af en kopi af de behandlede personoplysninger (artikel 4, nr. 3, i PIPA

([95]) Meddelelse nr. 2021-5, afsnit 3, nr. ii) (bilag I).

([96]) I henhold til artikel 35, stk. 3, i PIPA sammenholdt med artikel 42, stk. 2, i PIPA-gennemførelsesdekretet kan den dataansvarlige udsætte adgangen, hvis der er en »god grund« (dvs. berettigede årsager, f.eks. hvis der er behov for mere tid til at vurdere, om der kan gives adgang), men den dataansvarlige skal underrette den registrerede om en sådan begrundelse inden for 10 dage og oplyse, hvordan denne afgørelse kan påklages, og så snart grunden til udsættelse ikke længere er til stede, skal der gives adgang.

sammenholdt med artikel 41, stk. 1, i PIPA-gennemførelsesdekretet) ([97]). Adgangen kan kun begrænses (delvis adgang) ([98]) eller nægtes, hvis dette er fastsat ved lov ([99]), eller hvis den sandsynligvis vil skade tredjemands liv eller legeme eller er en uberettiget krænkelse af en anden persons ejendom og andre interesser (artikel 35, stk. 4, i PIPA) ([100]). Sidstnævnte indebærer, at der skal foretages en afvejning mellem den enkeltes og andres forfatningsmæssigt beskyttede rettigheder og friheder. Hvis adgangen begrænses eller nægtes, skal den dataansvarlige underrette den registrerede om årsagerne hertil og om, hvordan afgørelsen kan påklages (artikel 41, stk. 5, og artikel 42, stk. 2, i PIPA-gennemførelsesdekretet).

(77) For det andet har registrerede ret til at få deres personoplysninger berigtiget eller slettet ([101]), »medmindre andet er udtrykkeligt fastsat i andre love« (artikel 36, stk. 1 og 2, i PIPA) ([102]). Efter modtagelse af en anmodning skal den dataansvarlige straks undersøge sagen, træffe de nødvendige foranstaltninger ([103]) og underrette den registrerede herom inden for 10 dage. Hvis anmodningen ikke kan imødekommes, indebærer dette krav om underretning, at der skal oplyses om årsagerne til afslaget og om, hvordan afgørelsen kan påklages (jf. artikel 36, stk. 4, i PIPA sammenholdt med artikel 43, stk. 3, i PIPA-gennemførelsesdekretet) ([104]).

(78) Endelig har registrerede ret til straks at suspendere behandlingen af deres personoplysninger ([105]), medmindre en af de opregnede undtagelser finder anvendelse (artikel 37, stk. 1 og 2, i PIPA) ([106]). Den dataansvarlige kan afslå anmodningen, 1) hvis der er særlig lovhjemmel hertil, eller hvis det er nødvendigt (»uundgåeligt«) for at opfylde retlige forpligtelser, 2) hvis en suspension sandsynligvis vil skade tredjemands liv eller legeme eller er en uberettiget krænkelse af en anden persons ejendom og andre interesser, 3) hvis det ville være umuligt for en offentlig institution at udføre sin funktion i henhold til lovgivningen uden at behandle oplysningerne, eller 4) hvis den registrerede ikke udtrykkeligt opsiger den underliggende kontrakt med den dataansvarlige, selv om det ville være praktisk umuligt at gennemføre kontrakten uden at behandle oplysningerne. I så fald skal den dataansvarlige straks underrette den registrerede om årsagerne til afslaget og om, hvordan afgørelsen kan påklages (artikel 37, stk. 2, i PIPA sammenholdt med artikel 44, stk. 2, i PIPA-gennemførelsesdekretet). I henhold til artikel 37, stk. 4, i PIPA skal den dataansvarlige straks »træffe de nødvendige foranstaltninger, herunder tilintetgørelse af de relevante personoplysninger«, når pågældende efterkommer anmodningen om suspension ([107]).

(79) Retten til suspension gælder også, når personoplysninger anvendes til direkte markedsføring, dvs. med henblik på at markedsføre varer eller tjenesteydelser eller udbyde dem til salg. Desuden kræver en sådan viderebehandling

([97]) Adgang til personoplysninger, der behandles af en offentlig institution, kan indhentes direkte fra institutionen eller indirekte ved at indgive en anmodning til PIPC, som straks videresender anmodningen (artikel 35, stk. 2, i PIPA og artikel 41, stk. 3, i PIPA-gennemførelsesdekretet).

([98]) I henhold til artikel 42, stk. 1, i PIPA-gennemførelsesdekretet er den dataansvarlige forpligtet til at give delvis adgang, hvis i det mindste en del af oplysningerne ikke er omfattet af begrundelsen for afslaget.

([99]) Den grundlæggende ret til privatlivets fred og databeskyttelse samt de principper om nødvendighed og proportionalitet, der er fastsat i den koreanske forfatning, skal respekteres i denne lovgivning.

([100]) Offentlige institutioner kan desuden nægte at give adgang, hvis dette ville medføre alvorlige vanskeligheder i forbindelse med udførelsen af visse funktioner, herunder løbende revisioner eller pålæggelse, opkrævning eller tilbagebetaling af skatter (artikel 35, stk. 4, i PIPA).

([101]) I så fald skal den dataansvarlige træffe foranstaltninger, der forhindrer genoprettelsen af personoplysningerne, jf. artikel 36, stk. 3, i PIPA.

([102]) Sådanne love skal opfylde kravene i forfatningen om, at en grundlæggende rettighed kun kan begrænses, når det er nødvendigt af hensyn til den nationale sikkerhed eller opretholdelsen af lov og orden og den offentlige velfærd, og ikke må berøre frihedens eller rettighedens væsentligste indhold (forfatningens artikel 37, stk. 2).

([103]) Artikel 43, stk. 2, i PIPA-gennemførelsesdekretet indeholder bestemmelser om en særlig procedure, når den dataansvarlige behandler persondatafiler modtaget fra en anden dataansvarlig.

([104]) Undladelse af at træffe de nødvendige foranstaltninger til at berigtige eller slette personoplysninger og fortsat anvendelse eller videregivelse af disse oplysninger til tredjemand kan føre til strafferetlige sanktioner (artikel 73, stk. 2, i PIPA).

([105]) I henhold til artikel 44, stk. 2, i PIPA-gennemførelsesdekretet skal den dataansvarlige underrette den registrerede om, at den dataansvarlige behørigt har indstillet behandlingen inden for 10 dage fra modtagelsen af anmodningen.

([106]) I forhold til offentlige institutioner kan retten til suspension af behandlingen udøves i forbindelse med oplysninger i registrerede persondatafiler (artikel 37 sammenholdt med artikel 32 i PIPA). En sådan registrering er ikke påkrævet i et begrænset antal situationer, f.eks. hvis persondatafilerne vedrører nationale sikkerhedsspørgsmål, strafferetlige efterforskninger, diplomatiske forbindelser mv. (artikel 32, stk. 2, i PIPA).

([107]) Hvis behandlingen ikke suspenderes, kan det føre til strafferetlige sanktioner (artikel 73, stk. 3, i PIPA).

generelt den registreredes udtrykkelige (yderligere) samtykke (jf. artikel 15, stk. 1, nr. 1, og artikel 17, stk. 2, nr. 1, i PIPA) ([108]). I forbindelse med anmodningen om dette samtykke skal den dataansvarlige navnlig underrette den registrerede om den tilsigtede anvendelse af oplysningerne til direkte markedsføring — dvs. det forhold, at den registrerede kan kontaktes for at markedsføre varer eller tjenesteydelser eller udbyde dem til salg — på en »klart genkendelig måde« (artikel 22, stk. 2 og 4, i PIPA sammenholdt med artikel 17, stk. 2, nr. 1, i PIPA).

(80) For at lette udøvelsen af individuelle rettigheder skal den dataansvarlige indføre særlige procedurer og offentliggøre dem (artikel 38, stk. 4, i PIPA) ([109]). Dette omfatter procedurer for indsigelser mod afslag på en anmodning (artikel 38, stk. 5, i PIPA). Den dataansvarlige skal sikre, at proceduren for udøvelse af rettigheder er »brugervenlig i forhold til den registrerede« og ikke vanskeligere end proceduren for indsamling af personoplysninger. Dette omfatter også forpligtelsen til at give oplysninger om proceduren på dens websted (artikel 41, stk. 2, artikel 43, stk. 1, og artikel 44, stk. 1, i PIPA-gennemførelsesdekretet ([110])). Enkeltpersoner kan bemyndige en repræsentant til at indgive en sådan anmodning (artikel 38, stk. 1, i PIPA sammenholdt med artikel 45 i PIPA-gennemførelsesdekretet). Den dataansvarlige kan opkræve et gebyr (og i tilfælde af en anmodning om at sende kopier af personoplysninger, porto), men beløbet skal fastsættes »i forhold til de faktiske udgifter, der er nødvendige for behandlingen af [anmodningen]«. Der må ikke pålægges gebyrer (eller porto), hvis den dataansvarlige har foranlediget anmodningen (artikel 38, stk. 3, i PIPA sammenholdt med artikel 47 i PIPA-gennemførelsesdekretet).

(81) PIPA og gennemførelsesdekretet hertil indeholder ikke generelle bestemmelser, som vedrører beslutninger, der påvirker den registrerede, og som udelukkende bygger på automatisk behandling af personoplysninger. I forbindelse med personoplysninger, der er blevet indsamlet i Unionen, vil enhver beslutning baseret på automatisk behandling imidlertid typisk blive truffet af den dataansvarlige i Unionen (som har en direkte relation til den berørte registrerede), og den vil således være omfattet af forordning (EU) 2016/679 ([111]). Dette omfatter overførselsscenarier, hvor behandlingen foretages af en udenlandsk (f.eks. koreansk) erhvervsdrivende, der handler som mandatar (databehandler) på vegne af den dataansvarlige i Unionen (eller som en underdatabehandler, der handler på vegne af en databehandler i Unionen, som har modtaget oplysningerne fra den indsamlende dataansvarlige i Unionen), og som på dette grundlag således træffer beslutningen. Fraværet af specifikke regler om automatiske beslutninger i PIPA vil derfor sandsynligvis ikke have indvirkning på beskyttelsesniveauet for personoplysninger overført i henhold til denne afgørelse.

(82) Som en undtagelse finder bestemmelserne om gennemsigtighed efter anmodning (artikel 20) og individuelle rettigheder (artikel 35-37) samt kravet til udbydere af informations- og kommunikationstjenester om individuel underretning (artikel 39-8 i PIPA) ikke anvendelse på pseudonymiserede oplysninger, når disse behandles til statistiske formål, videnskabelige forskningsformål og arkivformål i samfundets interesse (artikel 28-7 i PIPA) ([112]). I overensstemmelse med tilgangen i artikel 11, stk. 2 (sammenholdt med betragtning 57) i forordning (EU) 2016/679 er dette begrundet i, at den dataansvarlige for at sikre gennemsigtighed eller indrømme individuelle rettigheder skulle fastslå, om nogle (og i givet fald hvilke) af oplysningerne vedrører den person, der fremsætter anmodningen, hvilket er udtrykkeligt forbudt i henhold til PIPA (artikel 28-5, stk. 1, i PIPA). Hvis en sådan genidentifikation indebærer, at pseudonymiseringen ophæves for hele det (pseudonymiserede) datasæt, vil det udsætte alle andre berørte personers personoplysninger for øgede risici. I forordning (EU) 2016/679 henvises til situationer, hvor genidentifikation er praktisk umulig, men tilgangen i PIPA er strengere ved udtrykkeligt at forbyde genidentifikation i alle situationer, hvor pseudonymiserede oplysninger behandles.

(83) Det koreanske system som beskrevet i betragtning 74-82 indeholder derfor regler om registreredes rettigheder, der sikrer et beskyttelsesniveau, som i det væsentlige svarer til det niveau, der er fastsat i forordning (EU) 2016/679.

([108]) Tvistbilæggelsesudvalget (jf. betragtning 133) har behandlet adskillige sager, hvor enkeltpersoner klagede over anvendelsen af deres oplysninger til direkte markedsføring uden samtykke, hvilket f.eks. har ført til, at den pågældende dataansvarlige har betalt erstatning og slettet personoplysninger (jf. f.eks. Tvistbilæggelsesudvalget 20R10-024(2020.11.18), 20R08-015(2020,8,28) og 20R07-031(2020.9.1)).

([109]) Se også artikel 30, stk. 1, nr. 5, i PIPA om politikken for beskyttelse af privatlivets fred, som bl.a. skal indeholde oplysninger om den enkeltes rettigheder og om, hvordan de udøves.

([110]) Se også artikel 39-7, stk. 2, i PIPA om udbydere af informations- og kommunikationstjenester.

([111]) I de ekstraordinære tilfælde, hvor den koreanske erhvervsdrivende har en direkte relation til den registrerede i EU, vil det omvendt typisk være en konsekvens af, at den erhvervsdrivende har rettet sin indsats mod den pågældende person i Den Europæiske Union ved at tilbyde denne varer eller tjenesteydelser eller ved at overvåge dennes adfærd. I dette scenarie vil den koreanske erhvervsdrivende selv være omfattet af reglerne i forordning (EU) 2016/679 (artikel 3, stk. 2) og således skulle overholde EU's databeskyttelseslovgivning.

([112]) Se også meddelelse nr. 2021-5, som bekræfter, at afdeling III i PIPA (herunder artikel 28-7) kun finder anvendelse, når pseudonymiserede oplysninger behandles til statistiske formål, videnskabelige forskningsformål og arkivformål i samfundets interesse, jf. afsnit 4 i bilag I til denne afgørelse.

2.3.9. *Videreoverførsel*

(84) Beskyttelsesniveauet for personoplysninger, der overføres fra Unionen til dataansvarlige i Republikken Korea, må ikke undermineres af videreoverførsel af sådanne oplysninger til modtagere i et tredjeland.

(85) Sådanne »videreoverførsler« udgør internationale overførsler fra Republikken Korea set fra den koreanske dataansvarliges synspunkt. I denne forbindelse skelner PIPA mellem outsourcing af behandling til outsourcingpartneren (dvs. en databehandler) og videregivelse af personoplysninger til tredjemand ([113]).

(86) For det første skal den koreanske dataansvarlige, når behandlingen af personoplysninger outsources til en enhed i et tredjeland, sikre, at PIPA's bestemmelser om outsourcing overholdes (artikel 26 i PIPA). Dette omfatter indførelse af et retligt bindende instrument, der bl.a. begrænser outsourcingpartnerens behandling til formålet med det outsourcede arbejde, pålægger tekniske og ledelsesmæssige garantier og begrænser den outsourcede behandling (jf. artikel 26, stk. 1, i PIPA), og offentliggørelse af oplysninger om det outsourcede arbejde. Desuden er den dataansvarlige forpligtet til at »uddanne« outsourcingpartneren i de nødvendige sikkerhedsforanstaltninger og føre tilsyn med, herunder gennem inspektioner, om alle den dataansvarliges forpligtelser i henhold til PIPA ([114]) og outsourcingkontrakten overholdes.

(87) Hvis outsourcingpartneren forvolder skade som følge af behandling af personoplysninger i strid med PIPA, holdes den dataansvarlige ansvarlig for denne skade med henblik på erstatningsansvar, som det er tilfældet med skade forvoldt af den dataansvarliges ansatte (artikel 26, stk. 6, i PIPA). Den koreanske dataansvarlige er derfor fortsat ansvarlig for de personoplysninger, der er blevet outsourcet, og skal sikre, at den udenlandske databehandler behandler oplysningerne i overensstemmelse med PIPA. Hvis outsourcingpartneren behandler oplysningerne i strid med PIPA, kan den koreanske dataansvarlige holdes ansvarlig for manglende overholdelse af sin forpligtelse til at sikre, at PIPA overholdes, f.eks. gennem dens tilsyn med outsourcingpartneren. Garantierne i outsourcingkontrakten og den koreanske dataansvarliges ansvar for outsourcingpartnerens handlinger sikrer kontinuitet i beskyttelsen, når behandlingen af personoplysninger outsources til en enhed uden for Korea.

(88) For det andet kan koreanske dataansvarlige videregive personoplysninger til en tredjemand, der befinder sig uden for Korea. Selv om PIPA indeholder en række retlige grunde, der giver mulighed for videregivelse til tredjemand generelt, skal den dataansvarlige, hvis tredjemand befinder sig uden for Korea, i princippet ([115]) indhente den registreredes samtykke ([116]) efter at have givet den registrerede oplysninger om 1) typen af personoplysninger, 2) modtageren af personoplysningerne, 3) formålet med videregivelsen, dvs. modtagerens formål med behandlingen, 4) opbevaringsperioden i forbindelse med modtagerens behandling samt 5) den registreredes ret til at nægte samtykke (artikel 17, stk. 2 og 3, i IPA). Det angives i meddelelse nr. 2021-5, afsnittet om gennemsigtighed (jf. betragtning 70), at enkeltpersoner skal informeres om det tredjeland, som deres oplysninger vil blive videregivet til. Dette sikrer, at registrerede i Unionen kan træffe en fuldt informeret beslutning om, hvorvidt de ønsker at give samtykke til en grænseoverskridende overførsel. Desuden må den dataansvarlige ikke indgå en aftale med tredjepartsmodtageren i strid med PIPA, hvilket betyder, at aftalen ikke må indeholde forpligtelser, der er i modstrid med de krav, som PIPA pålægger den dataansvarlige ([117]).

([113]) Der gælder særlige regler for udbydere af informations- og kommunikationstjenester. I henhold til artikel 39-12 i PIPA skal udbydere af informations- og kommunikationstjenester i princippet indhente brugerens samtykke til enhver grænseoverskridende overførsel af personoplysninger. Hvis personoplysninger overføres som led i outsourcingen af behandlingsaktiviteter, herunder til opbevaring, kræves der ikke samtykke, hvis de pågældende personer er blevet informeret direkte eller ved offentlig meddelelse på en sådan måde, at der forud herfor er let adgang til nærmere oplysninger om 1) de oplysninger, der skal overføres, 2) det land, som oplysningerne vil blive overført til (samt overførselsdato og -metode), 3) modtagerens navn og 4) formålet med modtagerens anvendelse og opbevaring (artikel 39-12, stk. 3, i PIPA). Desuden vil de generelle krav til outsourcing finde anvendelse i dette tilfælde. For hver overførsel skal der indføres særlige garantier med hensyn til sikkerhed, behandling af klager og tvister samt andre nødvendige foranstaltninger til at beskytte brugernes oplysninger (artikel 48-10 i PIPA-gennemførelsesdekretet).

([114]) Se også artikel 26, stk. 7, i PIPA, ifølge hvilken artikel 15-25, 27-31, 33-38 og 50 finder tilsvarende anvendelse på databehandleren.

([115]) Udbydere af informations- og kommunikationstjenester, der videregiver brugernes personoplysninger til tredjemand, skal altid indhente brugerens samtykke (artikel 39-12, stk. 2, i PIPA).

([116]) Som forklaret nærmere i fodnote 51 skal et sådant samtykke være frivilligt, informeret og specifikt, for at det kan være gyldigt.

([117]) Se også artikel 39-12, stk. 1, i PIPA om udbydere af informations- og kommunikationstjenester.

(89) Personoplysninger kan videregives til tredjemand (i udlandet) uden den registreredes samtykke, hvis formålet med videregivelsen forbliver »inden for rammer, der er rimeligt relateret til det oprindelige formål med indsamlingen« (artikel 17, stk. 4, i PIPA, jf. betragtning 36). Ved afgørelsen af, om der skal videregives personoplysninger til et »relateret« formål, skal den dataansvarlige imidlertid tage hensyn til, om videregivelsen er til ulempe for den registrerede, og om der er truffet de nødvendige sikkerhedsforanstaltninger (f.eks. kryptering). Da det tredjeland, som personoplysninger overføres til, ikke altid har et beskyttelsesniveau, som svarer til niveauet i PIPA, anerkendes det i afsnit 2 i meddelelse nr. 2021-5, at sådanne ulemper kan opstå og kun kan undgås, hvis den koreanske dataansvarlige og den udenlandske modtager gennem et retligt bindende instrument (f.eks. en kontrakt) sikrer et beskyttelsesniveau, som svarer til niveauet i PIPA, herunder med hensyn til registreredes rettigheder.

(90) Der gælder særlige regler for »ikkeformålsbestemt« videregivelse, dvs. videregivelse af oplysninger til tredjemand til et nyt (ikkerelateret) formål, som kun kan finde sted af en af grundene i artikel 18, stk. 2, i PIPA, jf. betragtning 39. Selv under disse omstændigheder er videregivelse til tredjemand imidlertid udelukket, hvis det er sandsynligt, at det vil »krænke den registreredes eller tredjemands interesser uretmæssigt«, hvilket kræver en afvejning af interesser. Desuden skal den dataansvarlige i henhold til artikel 18, stk. 5, i PIPA anvende yderligere garantier, hvilket kan omfatte at anmode tredjemand om at begrænse formålet med og metoden til behandling eller indføre specifikke sikkerhedsforanstaltninger. Da det tredjeland, som personoplysninger overføres til, ikke altid har et beskyttelsesniveau, som svarer til niveauet i PIPA, anerkendes det i afsnit 2 i meddelelse nr. 2021-5, at en sådan uberettiget krænkelse af den registreredes eller tredjemands interesser kan finde sted og kun kan undgås, hvis den koreanske dataansvarlige og den udenlandske modtager gennem et retligt bindende instrument (f.eks. en kontrakt) sikrer et beskyttelsesniveau, som svarer til niveauet i PIPA, herunder med hensyn til registreredes rettigheder.

(91) Reglerne i betragtning 86-90 sikrer derfor fortsat beskyttelse, når personoplysninger videreoverføres (til en »outsourcingpartner« eller tredjemand) fra Republikken Korea på en måde, som i det væsentlige svarer til det niveau, der er fastsat i forordning (EU) 2016/679.

2.3.10. *Ansvarlighed*

(92) I henhold til princippet om ansvarlighed skal enheder, der behandler oplysninger, træffe passende organisatoriske foranstaltninger med henblik på effektiv overholdelse af deres databeskyttelsesforpligtelser, og de skal være i stand til at dokumentere denne overholdelse, navnlig over for den kompetente tilsynsmyndighed.

(93) I henhold til artikel 3, stk. 6 og 8, i PIPA, skal den dataansvarlige behandle personoplysninger »på en måde, der minimerer risikoen for at krænke« den registreredes ret til privatlivets fred, og bestræbe sig på at vinde de registreredes tillid ved at overholde og udføre de opgaver og ansvarsområder, der er fastsat i PIPA og andre relaterede love. Dette omfatter udarbejdelse af en intern forvaltningsplan (artikel 29 i PIPA) samt passende uddannelse af og tilsyn med personalet (artikel 28 i PIPA).

(94) Som et middel til at sikre ansvarlighed pålægger artikel 31 i PIPA sammen med artikel 32 i PIPA-gennemførelsesdekretet de dataansvarlige en forpligtelse til at udpege en databeskyttelsesansvarlig med »overordnet ansvar for behandlingen af personoplysninger«. Denne databeskyttelsesansvarlige skal navnlig varetage følgende opgaver: 1) udarbejdelse og gennemførelse af en plan for beskyttelse af personoplysninger og udarbejdelse af en politik for beskyttelse af privatlivets fred, 2) gennemførelse af regelmæssige undersøgelser af status for og praksis for behandling af personoplysninger med henblik på at afhjælpe eventuelle mangler, 3) klagebehandling og afhjælpning, 4) oprettelse af et internt kontrolsystem for at forhindre videregivelse, misbrug eller forkert anvendelse af personoplysninger, 5) forberedelse og gennemførelse af et uddannelsesprogram, 6) beskyttelse, kontrol og forvaltning af persondatafiler og 7) tilintetgørelse af personoplysninger, når formålet med behandlingen er opfyldt eller opbevaringsperioden udløbet. Under udførelsen af disse opgaver kan den databeskyttelsesansvarlige kontrollere status for behandling af personoplysninger og relaterede systemer og anmode om oplysninger herom (artikel 31, stk. 3, i PIPA). Hvis den databeskyttelsesansvarlige bliver opmærksom på en overtrædelse af PIPA eller andre relevante databeskyttelseslove, træffer vedkommende straks korrigerende foranstaltninger og underretter den dataansvarliges ledelse (»lederen«) om disse foranstaltninger, hvis det er nødvendigt (artikel 31, stk. 4, i PIPA). I henhold til artikel 31, stk. 5, i PIPA må det ikke være forbundet med uberettigede ulemper for den databeskyttelsesansvarlige at varetage disse opgaver.

(95) Dataansvarlige skal desuden proaktivt bestræbe sig på at foretage en konsekvensanalyse vedrørende beskyttelse af privatlivets fred, hvis behandlingen af persondatafiler indebærer en risiko for privatlivets fred (artikel 33, stk. 8, i PIPA). På grundlag af artikel 33, stk. 1 og 2, i PIPA sammenholdt med artikel 35, 36 og 38 i PIPA-gennemførelsesdekretet vil faktorer såsom typen og karakteren af de behandlede oplysninger (navnlig om de udgør følsomme oplysninger), omfanget heraf, opbevaringsperioden og sandsynligheden for brud på datasikkerheden være relevante for vurderingen af graden af risiko for de registreredes rettigheder. Formålet med konsekvensanalysen vedrørende beskyttelse af privatlivets fred er at sikre, at risikofaktorerne for privatlivets fred og eventuelle sikkerheds- eller andre modforanstaltninger analyseres, og at påpege forhold, der skal forbedres (jf. artikel 33, stk. 1, i PIPA sammenholdt med artikel 38 i PIPA-gennemførelsesdekretet).

(96) Offentlige institutioner er forpligtet til at foretage en konsekvensanalyse i forbindelse med behandlingen af visse persondatafiler, hvor risikoen for krænkelser af privatlivets fred er højere (artikel 33, stk. 1, i PIPA). I overensstemmelse med artikel 35 i PIPA-gennemførelsesdekretet er dette bl.a. tilfældet for filer med følsomme oplysninger om mindst 50 000 registrerede, filer, som vil blive matchet med andre filer og som følge heraf vil indeholde oplysninger om mindst 500 000 registrerede, eller filer med oplysninger om mindst en million registrerede. Resultatet af en konsekvensanalyse foretaget af en offentlig institution skal meddeles PIPC (artikel 33, stk. 1, i PIPA), som kan afgive udtalelse (artikel 33, stk. 3, i PIPA).

(97) Endelig fastsættes det i artikel 13 i PIPA, at PIPC fastlægger de fornødne politikker til at fremme og støtte de dataansvarliges »selvregulerende databeskyttelsesaktiviteter«, bl.a. gennem uddannelse i databeskyttelse, fremme af og støtte til organisationer, der beskæftiger sig med databeskyttelse, og ved at bistå dataansvarlige med at indføre og gennemføre selvreguleringsordninger. PIPC skal desuden indføre og lette ePRIVACY Mark-systemet. I den forbindelse giver artikel 32-2 i PIPA sammen med artikel 34-2 til 34-8 i PIPA-gennemførelsesdekretet mulighed for at certificere, at den dataansvarliges systemer til behandling og beskyttelse af personoplysninger opfylder kravene i PIPA. I henhold til disse regler ([118]) kan den dataansvarlige certificeres (for en periode på tre år), hvis denne opfylder de certificeringskriterier, der er fastsat af PIPC, herunder om etablering af ledelsesmæssige, tekniske og fysiske garantier for beskyttelse af personoplysninger ([119]). PIPC skal undersøge den dataansvarliges systemer af relevans for certificeringen mindst én gang om året for at sikre, at ordningen fortsat er effektiv, hvilket kan indebære, at certificeringen tilbagekaldes (artikel 32, stk. 4, i PIPA sammenholdt med artikel 34-5 i PIPA-gennemførelsesdekretet, såkaldt »opfølgningsstyring«).

(98) Den koreanske ramme gennemfører derfor princippet om ansvarlighed på en måde, der sikrer et beskyttelsesniveau, som i det væsentlige svarer til det niveau, der er fastsat i forordning (EU) 2016/679, herunder gennem indførelse af forskellige mekanismer til at sikre og påvise overholdelsen af PIPA.

2.3.11. *Særlige regler for behandling af personlige kreditoplysninger*

(99) Som beskrevet i betragtning 13 fastsætter CIA særlige regler for kommercielle operatørers behandling af personlige kreditoplysninger. Ved behandling af personlige kreditoplysninger skal kommercielle operatører derfor overholde de generelle krav i PIPA, medmindre CIA indeholder mere specifikke regler. Dette vil f.eks. være tilfældet, når de behandler oplysninger vedrørende et kreditkort eller en bankkonto i forbindelse med en handelstransaktion med en person. Som sektorspecifik lovgivning om behandling af kreditoplysninger (både personoplysninger og ikkepersonoplysninger) fastsætter CIA ikke blot specifikke databeskyttelsesgarantier (f.eks. for gennemsigtighed og sikkerhed), men regulerer også mere generelt de specifikke omstændigheder, hvorunder personoplysninger kan behandles. Dette afspejles især i de detaljerede krav til anvendelse, videregivelse af oplysninger til tredjemand og opbevaring af sådanne oplysninger.

(100) I lighed med PIPA afspejler CIA legalitetsprincippet og proportionalitetsprincippet. For det første giver artikel 15, stk. 1, i CIA som et generelt krav kun mulighed for at indsamle personlige kreditoplysninger på rimelige og retfærdige måder og i mindst muligt omfang for at nå et tilsigtet formål i overensstemmelse med artikel 3, stk. 1-2, i PIPA. For det andet regulerer CIA specifikt lovligheden af behandlingen af personlige kreditoplysninger ved at begrænse indsamlingen, anvendelsen og videregivelsen heraf til tredjemand og generelt knytte disse behandlingsaktiviteter til kravet om den berørte persons samtykke.

([118]) Hvis den dataansvarlige ønsker at henvise til eller fremme certificeringen i forbindelse med sine forretningsaktiviteter, kan den dataansvarlige desuden anvende det mærke for beskyttelse af personoplysninger, som PIPC har indført. Jf. artikel 34-7 i PIPA-gennemførelsesdekretet.

([119]) Siden november 2018 er der udviklet et system til forvaltning af personoplysninger og informationssikkerhed (ISMS-P), som certificerer, at de dataansvarlige har indført et omfattende forvaltningssystem.

(101) Personlige kreditoplysninger kan indsamles af en af de grunde, der er fastsat i PIPA, eller af specifikke grunde fastsat i CIA. Da artikel 45 i forordning (EU) 2016/679 forudsætter, at personoplysningerne videregives af en dataansvarlig eller databehandler i Unionen, men ikke omfatter den koreanske dataansvarliges direkte indsamling (f.eks. fra den berørte person eller et websted), er det kun samtykke og de grunde, der er fastsat i PIPA, som er relevante for denne afgørelse. Disse grunde omfatter navnlig situationer, hvor videregivelsen er nødvendig for at opfylde en kontrakt med den registrerede eller for den koreanske dataansvarliges forfølgelse af en legitim interesse (artikel 15, stk. 1, nr. 4 og 6, i PIPA ([120])).

(102) Når de personlige kreditoplysninger er indsamlet, kan de anvendes 1) til det oprindelige formål, hvortil de blev givet direkte af den pågældende person ([121]), 2) til et formål, der er foreneligt med det oprindelige formål med indsamlingen ([122]), 3) til at vurdere, om den forretningsforbindelse, som den pågældende person har anmodet om, skal etableres eller opretholdes ([123]), 4) til statistiske formål, videnskabelige forskningsformål og arkivformål i samfundets interesse ([124]), hvis oplysningerne er pseudonymiserede ([125]), 5) hvis der opnås yderligere samtykke, eller 6) i overensstemmelse med lovgivningen.

(103) Hvis en kommerciel operatør ønsker at videregive personlige kreditoplysninger til tredjemand, skal operatøren indhente den registreredes samtykke ([126]) efter at have underrettet den pågældende om modtageren af oplysningerne og formålet med behandlingen af oplysningerne, om hvilke oplysninger der skal videregives, og om opbevaringsperioden hos modtageren og retten til at nægte samtykke (artikel 32, stk. 1, i CIA, og artikel 28, stk. 2), i CIA-gennemførelsesdekretet ([127]). Dette krav om samtykke finder ikke anvendelse i specifikke situationer, hvor der videregives personlige kreditoplysninger ([128]): 1) til en outsourcingpartner med henblik på outsourcing ([129]), 2) til tredjemand i tilfælde af virksomhedsoverdragelse, spaltning eller fusion, 3) til statistiske formål, videnskabelige forskningsformål og arkivformål i samfundets interesse, hvis oplysningerne er pseudonymiserede, 4) til et formål, der er foreneligt med det oprindelige formål med indsamlingen, 5) til en tredjemand, der anvender oplysningerne til at inddrive en fordring på den pågældende ([130]), 6) for at efterkomme en retskendelse, 7) til en anklager eller kriminalpolitiet i en nødsituation, hvis den pågældendes liv er i fare, eller hvis

([120]) CIA indeholder også andre retsgrundlag for indsamling, dvs. hvor det er påkrævet ved lov, hvor oplysningerne offentliggøres af en offentlig institution i henhold til lovgivningen om informationsfrihed, eller hvor oplysningerne er tilgængelige på et socialt netværk. Hvis den kommercielle operatør skal kunne påberåbe sig den sidste grund, skal operatøren kunne påvise, at indsamlingen forbliver inden for rammerne af den registreredes samtykke på grundlag af en rimelig (»objektiv«) fortolkning og under hensyntagen til oplysningernes karakter, hensigten og formålet med at stille oplysningerne til rådighed på det sociale netværk, og om formålet med indsamlingen er »yderst relevant« for dette formål mv. (artikel 13 i CIA-gennemførelsesdekretet). Som forklaret i betragtning 101 vil disse grunde imidlertid i princippet ikke være relevante i et overførselsscenarie.

([121]) Når kreditoplysninger frembringes eller videregives i forbindelse med en kommerciel transaktion med den pågældende person. Denne begrundelse kan imidlertid ikke påberåbes med henblik på at anvende personlige kreditoplysninger til direkte markedsføring (jf. artikel 33, stk. 1, nr. 3, i CIA).

([122]) For at afgøre, om formålet med anvendelsen er foreneligt med det oprindelige formål med indsamlingen, skal følgende faktorer tages i betragtning: 1) forholdet (»relevans«) mellem de to formål, 2) den måde, hvorpå oplysningerne er indsamlet, 3) indvirkningen af anvendelsen på den pågældende person, og 4) om passende sikkerhedsforanstaltninger såsom pseudonymisering er blevet gennemført (jf. artikel 32, stk. 6, nr. 9-4, i CIA).

([123]) En dataansvarlig kan f.eks. være nødt til at tage hensyn til personlige kreditoplysninger, som vedkommende har modtaget fra en person, for at afgøre, om lånet til den pågældende skal forlænges.

([124]) Artikel 33 i CIA sammenholdt med artikel 32, stk. 6, nr. 9-2, 9-4 og 10, i CIA.

([125]) Pseudonymisering defineres i artikel 2, stk. 15, i CIA som behandling af personlige kreditoplysninger på en sådan måde, at enkeltpersoner ikke længere kan identificeres ud fra oplysningerne, medmindre de samkøres med supplerende oplysninger. Selv om CIA indeholder specifikke garantier for behandling af pseudonymiserede oplysninger til statistiske formål, videnskabelige forskningsformål og arkivformål i samfundets interesse (artikel 40-2 i CIA), finder disse regler ikke anvendelse på kommercielle organisationer. Sidstnævnte er i stedet fortsat underlagt de specifikke krav i afdeling III i PIPA, jf. betragtning 42-48. Artikel 40-3 i CIA fritager desuden behandling af pseudonymiserede kreditoplysninger — til statistiske formål, videnskabelige forskningsformål og arkivformål i samfundets interesse — fra kravene om gennemsigtighed og individuelle rettigheder i lighed med undtagelsen i artikel 28-7 i PIPA og med forbehold af garantierne i afdeling III i PIPA som nærmere beskrevet i betragtning 42-48.

([126]) Dette gælder ikke, hvis oplysningerne videregives til tredjemand for at sikre, at de personlige kreditoplysninger er korrekte og ajourførte, så længe videregivelsen finder sted inden for rammerne af det oprindelige formål med behandlingen (artikel 32, stk. 1, i CIA). Dette kan f.eks. forekomme, når der videregives ajourførte oplysninger til et kreditvurderingsbureau for at sikre, at dets optegnelser er korrekte.

([127]) Hvis det ikke er praktisk muligt at videregive ovennævnte oplysninger, kan det være tilstrækkeligt at anmode den registrerede om at rette henvendelse til tredjepartsmodtageren og give de krævede oplysninger.

([128]) Da CIA ikke specifikt regulerer videregivelse af personlige kreditoplysninger til udlandet, skal denne videregivelse være i overensstemmelse med de garantier for videreoverførsel, der er fastsat i afsnit 2 i meddelelse nr. 2021-5.

([129]) Outsourcing af behandlingen af personlige kreditoplysninger må kun finde sted på grundlag af en skriftlig aftale og i overensstemmelse med kravene i artikel 26, stk. 1-3 og 5, i PIPA som beskrevet i betragtning 20 (artikel 17 i CIA og artikel 14 i CIA-gennemførelsesdekretet). Outsourcingpartneren må kun anvende oplysningerne inden for rammerne af de outsourcede forpligtelser, og outsourceren skal indføre særlige sikkerhedskrav (f.eks. kryptering) og oplyse outsourcingpartneren om, hvordan det kan forhindres, at kreditoplysningerne går tabt, stjæles, videregives, ændres eller kompromitteres.

([130]) Se også artikel 28, stk. 10, nr. 1, 2 og 6, i CIA-gennemførelsesdekretet.

den pågældende forventes at lide legemsbeskadigelse, og der ikke er tid til at udstede en retskendelse ([131]), 8) til de kompetente skattemyndigheder for at overholde skattelovgivningen eller 9) i overensstemmelse med anden lovgivning. I tilfælde af videregivelse af en af disse grunde skal den registrerede underrettes herom på forhånd (artikel 32, stk. 7, i CIA).

(104) CIA regulerer også specifikt varigheden af behandlingen af personlige kreditoplysninger af en af disse grunde til anvendelse eller videregivelse til tredjemand efter afslutningen af forretningsforholdet med den pågældende ([132]). Kun de oplysninger, der var nødvendige for at etablere eller opretholde dette forhold, kan opbevares, hvis der gives supplerende garantier (de skal holdes adskilt fra kreditoplysninger, der vedrører personer, med hvem der består et forretningsforhold, som er beskyttet af specifikke sikkerhedsforanstaltninger, og som kun er tilgængelige for bemyndigede personer) ([133]). Alle andre oplysninger skal slettes (artikel 17-2, stk. 1, nr. 2, i CIA-gennemførelsesdekretet). For at afgøre, hvilke oplysninger der var nødvendige for forretningsforholdet, skal der tages hensyn til forskellige faktorer, herunder om det ville have været muligt at etablere forholdet uden oplysningerne, og om det direkte vedrører de varer eller tjenesteydelser, der er leveret til den registrerede (artikel 17-2, stk. 2, i CIA-gennemførelsesdekretet).

(105) Selv i tilfælde, hvor personlige kreditoplysninger i princippet kan opbevares efter forretningsforholdets ophør, skal de slettes senest tre måneder efter opnåelsen af det videre formål med behandlingen ([134]) eller under alle omstændigheder efter fem år (artikel 20-2 i CIA). I et begrænset antal tilfælde kan personlige kreditoplysninger opbevares i mere end fem år, navnlig hvis det er nødvendigt for at opfylde en retlig forpligtelse, hvis det er nødvendigt for at beskytte en persons vitale interesser, liv, legeme eller ejendom, med henblik på arkivering af pseudonymiserede oplysninger (som blev anvendt til videnskabelige forskningsformål, statistiske formål og arkivformål i samfundets interesse) eller til forsikringsformål (navnlig til forsikringsbetalinger eller til forebyggelse af forsikringssvig) ([135]). I disse ekstraordinære tilfælde gælder der særlige garantier (f.eks. underretning af den registrerede om videreanvendelsen, adskillelse af de opbevarede oplysninger fra de oplysninger, der vedrører personer, med hvem der stadig består et forretningsforhold, begrænsning af adgangsrettigheder, jf. artikel 17-2, stk. 1-2, i CIA-gennemførelsesdekretet).

(106) CIA præciserer også principperne om nøjagtighed og datakvalitet ved at kræve, at personlige kreditoplysninger »registreres, ændres og forvaltes« for at sikre, at de er korrekte og ajourførte (artikel 18, stk. 1, i CIA, og artikel 15, stk. 3, i CIA-gennemførelsesdekretet) ([136]). Når kommercielle operatører giver kreditoplysninger til visse andre enheder (f.eks. kreditvurderingsbureauer), skal de også specifikt kontrollere oplysningernes nøjagtighed for at sikre, at modtageren kun registrerer og forvalter nøjagtige oplysninger (artikel 15, stk. 1, i CIA-gennemførelsesdekretet sammenholdt med artikel 18, stk. 1, i CIA). Mere generelt kræver CIA, at der føres fortegnelser over indsamling, anvendelse, videregivelse til tredjemand og tilintetgørelse af personlige kreditoplysninger (artikel 20, stk. 2, i CIA) ([137]).

(107) Behandlingen af personlige kreditoplysninger er desuden underlagt særlige datasikkerhedskrav. CIA kræver navnlig, at der gennemføres teknologiske, fysiske og organisatoriske foranstaltninger for at forhindre ulovlig adgang til computersystemer og ændring og tilintetgørelse af eller enhver anden risiko for de behandlede oplysninger (f.eks. ved hjælp af adgangskontrol, jf. artikel 19 i CIA og artikel 16 i CIA-gennemførelsesdekretet). Desuden skal der i forbindelse med udveksling af personlige kreditoplysninger med tredjemand indgås en aftale, der fastsætter specifikke sikkerhedsforanstaltninger (artikel 19, stk. 2, i CIA). I tilfælde af brud på datasikkerheden i forbindelse med personlige kreditoplysninger skal der træffes foranstaltninger til at minimere eventuel skade, og de berørte personer skal straks underrettes (artikel 39-4, stk. 1-2, i CIA). Desuden skal PIPC informeres om underretningen af de registrerede og om de foranstaltninger, der er blevet gennemført (artikel 39-4, stk. 4, i CIA).

([131]) I så fald skal der straks anmodes om en kendelse. Hvis kendelsen ikke udstedes inden for 36 timer, skal de modtagne oplysninger straks slettes (artikel 32, stk. 6, nr. 6, i CIA).

([132]) En af parterne har f.eks. udøvet sin opsigelsesret, da de kontraktlige forpligtelser er blevet opfyldt mv., jf. artikel 17-2, stk. 5, CIA-gennemførelsesdekretet.

([133]) Artikel 20-2, stk. 1, i CIA og artikel 17-2, stk. 1, nr. 1, i CIA-gennemførelsesdekretet.

([134]) Ved fastsættelsen af denne frist tages der højde for, at det ofte ikke vil være muligt at slette oplysningerne med det samme, da det typisk kræver visse trin (f.eks. adskillelse af de oplysninger, der skal slettes fra andre oplysninger, og sletning uden at påvirke informationssystemernes stabilitet), som tager nogen tid at gennemføre.

([135]) Artikel 20-2, stk. 2, i CIA.

([136]) I artikel 18, stk. 2, i CIA og artikel 15, stk. 4, i CIA-gennemførelsesdekretet fastsættes mere specifikke regler for dette registreringskrav, f.eks. for fortegnelser over oplysninger, der kan være til ulempe for en person, f.eks. oplysninger om kriminalitet og konkurs.

([137]) Med hensyn til andre ansvarlighedsmekanismer kræver CIA, at visse organisationer (f.eks. kooperativer og offentlige selskaber, jf. artikel 21, stk. 2, i CIA-gennemførelsesdekretet) udpeger en »kreditinformationsadministrator/rådgiver«, som er ansvarlig for at overvåge overholdelsen af CIA og varetager de opgaver, der påhviler »den databeskyttelsesansvarlige« i henhold til PIPA (artikel 20, stk. 3 og 4, i CIA).

(108) CIA pålægger også specifikke gennemsigtighedsforpligtelser i forbindelse med indhentning af samtykke til anvendelse eller videregivelse af personlige kreditoplysninger (artikel 32, stk. 4, og artikel 34-2 i CIA og artikel 30-3 i CIA-gennemførelsesdekretet) og mere generelt, inden der videregives oplysninger til tredjemand (artikel 32, stk. 7, i CIA) ([138]). Derudover har de registrerede ret til at anmode om oplysninger om anvendelsen og videregivelsen af deres kreditoplysninger til tredjemand i de tre år, der går forud for anmodningen (herunder om formålet med og datoerne for en sådan anvendelse/videregivelse) ([139]).

(109) I henhold til CIA har den registrerede også ret til at få indsigt i sine personlige kreditoplysninger (artikel 38, stk. 1, i CIA) og til at få berigtiget ukorrekte oplysninger (artikel 38, stk. 2-3, i CIA) ([140]). Ud over den generelle ret til sletning i henhold til PIPA (jf. betragtning 77) giver CIA desuden en specifik ret til at få slettet personlige kreditoplysninger, der er blevet opbevaret længere end i de opbevaringsperioder, der er nævnt i betragtning 104, dvs. fem år (for personlige kreditoplysninger, der var nødvendige for at etablere eller opretholde et forretningsforhold) eller tre måneder (for andre typer af personlige kreditoplysninger) ([141]). En anmodning om sletning kan undtagelsesvis afslås, hvis yderligere opbevaring er nødvendig under de omstændigheder, der er beskrevet i betragtning 105. Hvis en person anmoder om sletning, men en af undtagelserne finder anvendelse, skal der gælde særlige garantier for de pågældende kreditoplysninger (artikel 38-3, stk. 3, i CIA, og artikel 33-3 i CIA-gennemførelsesdekretet). F.eks. skal oplysningerne opbevares adskilt fra andre oplysninger, de må kun tilgås af en bemyndiget person og skal være omfattet af særlige sikkerhedsforanstaltninger.

(110) Ud over de rettigheder, der er nævnt i betragtning 109, garanterer CIA de registrerede en ret til at anmode en dataansvarlig om at ophøre med at kontakte dem med henblik på direkte markedsføring (artikel 37, stk. 2, i loven) og en ret til dataportabilitet. Med hensyn til sidstnævnte giver CIA de registrerede mulighed for at anmode om videregivelse af deres personlige kreditoplysninger til dem selv eller til visse tredjemænd (f.eks. finansielle institutioner og kreditvurderingsselskaber). De personlige kreditoplysninger skal behandles og videregives til tredjemand i et format, der kan behandles af en databehandlingsenhed (f.eks. en computer).

(111) I det omfang CIA indeholder specifikke regler i forhold til PIPA, mener Kommissionen derfor, at disse regler også sikrer et beskyttelsesniveau, som i det væsentlige svarer til det niveau, der er fastsat i forordning (EU) 2016/679.

2.4. **Tilsyn og håndhævelse**

(112) For at sikre, at et tilstrækkeligt databeskyttelsesniveau garanteres i praksis, bør der være oprettet en uafhængig tilsynsmyndighed med beføjelser til at overvåge og sikre, at databeskyttelsesreglerne overholdes. Denne myndighed bør være fuldstændig uafhængig og upartisk i udførelsen af sine opgaver og udøvelsen af sine beføjelser.

2.4.1. *Uafhængigt tilsyn*

(113) PIPC er den koreanske uafhængige myndighed med ansvar for tilsyn med og håndhævelse af PIPA. PIPC består af en formand, en næstformand og syv kommissærer. Formanden og næstformanden udnævnes af præsidenten efter indstilling fra premierministeren. To af kommissærerne udnævnes af præsidenten efter indstilling fra formanden og fem efter indstilling fra nationalforsamlingen (heraf to efter indstilling fra det politiske parti, som præsidenten tilhører, og tre efter indstilling fra andre politiske partier (artikel 7-2, stk. 2, PIPA), hvilket bidrager til at

([138]) Dette omfatter et generelt krav om underretning (artikel 32, stk. 7, i CIA) og en specifik gennemsigtighedsforpligtelse, hvis oplysninger, der gør det muligt at vurdere en persons kreditværdighed, videregives til visse enheder såsom kreditvurderingsbureauer og kreditoplysningsbureauer (artikel 35-3 i CIA og artikel 30-3 i CIA-gennemførelsesdekretet), eller hvis forretningsforhold ikke indgås eller afsluttes på grundlag af personlige kreditoplysninger modtaget fra tredjemand (artikel 36 i CIA og artikel 31 i CIA-gennemførelsesdekretet).

([139]) Artikel 35 i CIA. Visse kommercielle organisationer, f.eks. kooperativer og offentlige selskaber (artikel 21, stk. 2, i CIA-gennemførelsesdekretet), er underlagt yderligere gennemsigtighedskrav, f.eks. om at gøre visse oplysninger offentligt tilgængelige (artikel 31 i CIA) og om at informere de registrerede om mulige ulemper for deres kreditvurderingsscore, når de deltager i finansielle transaktioner, der udgør en kreditrisiko (artikel 35-2 i CIA).

([140]) Hvad angår betingelserne og undtagelserne fra retten til indsigt og berigtigelse, finder reglerne i PIPA (beskrevet i betragtning 76-77) anvendelse. Desuden er der fastsat yderligere bestemmelser i artikel 38, stk. 4-8, i CIA og artikel 33 i CIA-gennemførelsesdekretet. En kommerciel operatør, der har berigtiget eller slettet ukorrekte kreditoplysninger, skal navnlig underrette den registrerede herom. Desuden skal enhver tredjemand, til hvem disse oplysninger er blevet videregivet inden for de foregående seks måneder, underrettes, og den berørte registrerede skal underrettes herom. Hvis en person ikke er tilfreds med behandlingen af en anmodning om berigtigelse, kan vedkommende indgive en anmodning til PIPC, som kontrollerer den dataansvarliges handlinger og kan pålægge korrigerende foranstaltninger.

([141]) Artikel 38-3 i CIA.

modvirke partiskhed i udnævnelsesprocessen) ([142]). Denne procedure er i overensstemmelse med de krav, der gælder for udnævnelse af medlemmer af databeskyttelsesmyndigheder i Unionen (artikel 53, stk. 1, i forordning (EU) 2016/679). Alle kommissærer skal desuden afholde sig fra enhver indtægtsskabende erhvervsvirksomhed og politiske aktiviteter og må ikke bestride stillinger i den offentlige forvaltning eller nationalforsamlingen (artikel 7-6 og artikel 7-7, stk. 1, nr. 3, i PIPA) ([143]). Alle kommissærer er omfattet af særlige regler, som forhindrer dem i at deltage i forhandlinger i tilfælde af en mulig interessekonflikt (artikel 7-11 i PIPA). PIPC bistås af et sekretariat (artikel 7-13) og kan nedsætte underudvalg (bestående af tre kommissærer) til at håndtere mindre overtrædelser og tilbagevendende sager (artikel 7-12 i PIPA).

(114) Hvert medlem af PIPC udnævnes for tre år og kan genudnævnes én gang (artikel 7-4, stk. 1, i PIPA). Kommissærer kan kun afsættes under særlige omstændigheder, nemlig hvis de ikke længere er i stand til at varetage deres opgaver på grund af langvarig psykisk eller fysisk sygdom, handler i strid med loven eller opfylder en af grundene til udelukkelse fra embedet ([144]) (artikel 7-5 i PIPA). Dette giver dem institutionel beskyttelse i forbindelse med udøvelsen af deres funktioner.

(115) Mere generelt garanterer artikel 7, stk. 1, i PIPA udtrykkeligt PIPC's uafhængighed, og i henhold til artikel 7-5, stk. 2, i PIPA skal kommissærerne udføre deres opgaver uafhængigt og i overensstemmelse med lovgivningen og deres samvittighed ([145]). De beskrevne institutionelle og proceduremæssige garantier, herunder for udnævnelse og afsættelse af medlemmer, sikrer, at PIPC handler i fuld uafhængighed uden udefra kommende påvirkning eller instrukser. Som et centralt forvaltningsorgan foreslår PIPC desuden årligt sit eget budget (som gennemgås af finansministeriet som en del af det samlede nationale budget inden nationalforsamlingens vedtagelse), og PIPC har ansvaret for sin egen personaleforvaltning. PIPC's aktuelle budget udgør ca. 35 mio. EUR, og udvalget har 154 ansatte (herunder 40 medarbejdere med speciale i informations- og kommunikationsteknologi, 32 medarbejdere med fokus på undersøgelser og 40 juridiske eksperter).

(116) PIPC's opgaver og beføjelser er hovedsagelig fastsat i artikel 7-8 og 7-9 samt i artikel 61-66 i PIPA ([146]). PIPC's opgaver omfatter navnlig rådgivning om love og bestemmelser vedrørende databeskyttelse, udvikling af databeskyttelsespolitikker og -retningslinjer, undersøgelse af overtrædelser af individuelle rettigheder, behandling af klager og tvistbilæggelse, håndhævelse af overholdelse af PIPA, sikring af uddannelse i og fremme af databeskyttelse og udveksling og samarbejde med tredjelandes databeskyttelsesmyndigheder ([147]).

(117) På grundlag af artikel 68 i PIPA sammenholdt med artikel 62 i PIPA-gennemførelsesdekretet er visse af PIPC's opgaver blevet delegeret til Koreas internet- og sikkerhedsagentur: 1) uddannelse og PR, 2) uddannelse af specialister og udvikling af kriterier for konsekvensanalyser vedrørende beskyttelse af privatlivets fred, 3) behandling af anmodninger om udpegelse af institutioner, der foretager konsekvensanalyser vedrørende beskyttelse af privatlivets fred, 4) behandling af anmodninger om indirekte adgang til personoplysninger, der opbevares af offentlige myndigheder (artikel 35, stk. 2, i PIPA), og 5) opgaven med at anmode om materiale og foretage

([142]) Kun personer, der opfylder følgende kriterier, kan udnævnes til PIPC-kommissærer: Højtstående embedsmænd med ansvar for spørgsmål vedrørende personoplysninger, tidligere dommere, offentlige anklagere eller advokater, der har udøvet deres erhverv i mindst ti år, tidligere ledere med erfaring i databeskyttelse, der har arbejdet i en offentlig institution eller organisation i mere end tre år, eller som er blevet anbefalet af en sådan institution eller organisation, og tidligere lektorer med faglig viden inden for databeskyttelse, der har arbejdet mindst fem år i en akademisk institution (artikel 7-2 i PIPA).

([143]) Se også artikel 4-2 i PIPA-gennemførelsesdekretet.

([144]) Jf. artikel 7-7 i PIPA, ifølge hvilken ikkekoreanske statsborgere og medlemmer af politiske partier ikke kan blive medlemmer af PIPC. Det samme gælder for personer, som er blevet pålagt visse former for strafferetlige sanktioner, som er blevet fjernet fra embedet ved disciplinære foranstaltninger inden for de seneste fem år mv. (artikel 7-7 i PIPA sammenholdt med artikel 33 i lov om offentligt ansatte).

([145]) I artikel 7, stk. 2, i PIPA henvises til premierministerens generelle beføjelse i henhold til artikel 18 i lov om regeringens organisation til — med præsidentens godkendelse — at suspendere eller tilbagekalde enhver ulovlig eller uberettiget disposition truffet af et centralt forvaltningsorgan, men PIPC's undersøgelses- eller håndhævelsesbeføjelser omfatter ikke en sådan beføjelse (jf. artikel 7, stk. 2, nr. 1 og 2, i PIPA). Ifølge de forklaringer, der er modtaget fra den koreanske regering, har artikel 18 i lov om regeringens organisation til formål at give premierministeren mulighed for at handle under ekstraordinære omstændigheder, f.eks. for at mægle i en tvist mellem forskellige statslige organer. Premierministeren har imidlertid aldrig gjort brug af denne beføjelse, siden denne bestemmelse blev vedtaget i 1963.

([146]) Når det er nødvendigt for at varetage opgaverne i henhold til artikel 7-9, stk. 1, i PIPA, kan PIPC indhente udtalelser fra relevante offentlige ansatte, eksperter i databeskyttelse, civilsamfundsorganisationer og relevante erhvervsdrivende. Desuden kan PIPC anmode om relevant materiale, fremsætte henstillinger om forbedringer og kontrollere, om disse er gennemført (artikel 7-9, stk. 2-5, i PIPA).

([147]) Se også artikel 9 i PIPA (treårig masterplan for beskyttelse af personoplysninger), artikel 12 i PIPA (standardretningslinjer for beskyttelse af personoplysninger), artikel 13 i PIPA (politikker til fremme af og støtte for selvregulering).

inspektioner i forbindelse med klager, der modtages via det såkaldte callcenter for privatlivsbeskyttelse. I forbindelse med behandlingen af klager via callcentret for privatlivsbeskyttelse videregiver Koreas internet- og sikkerhedsagentur sagen til PIPC eller til anklagemyndigheden, hvis det finder, at loven er blevet overtrådt. Muligheden for at indgive en klage til callcentret for privatlivsbeskyttelse forhindrer ikke enkeltpersoner i at indgive en klage direkte til PIPC eller henvende sig til PIPC, hvis de mener, at deres klage ikke er blevet behandlet tilfredsstillende af Koreas internet- og sikkerhedsagentur.

2.4.2. *Håndhævelse, herunder sanktioner*

(118) For at sikre overholdelsen af PIPA har lovgiveren tildelt PIPC både undersøgelses- og håndhævelsesbeføjelser, lige fra beføjelser til at fremsætte henstillinger til at pålægge administrative bøder. Disse beføjelser suppleres af en ordning med strafferetlige sanktioner.

(119) For så vidt angår undersøgelsesbeføjelser kan PIPC, hvis der er mistanke om eller blevet indberettet en overtrædelse af PIPA, eller hvis det er nødvendigt for at beskytte de registreredes rettigheder mod overtrædelser, foretage inspektioner på stedet og anmode om alt relevant materiale (f.eks. genstande og dokumenter) fra de dataansvarlige (artikel 63 i PIPA sammenholdt med artikel 60 i PIPA-gennemførelsesdekretet) ([148]).

(120) Med hensyn til håndhævelse kan PIPC i henhold til artikel 61, stk. 2, i PIPA fremsætte henstillinger til de dataansvarlige om, hvordan beskyttelsen af personoplysninger i forbindelse med specifikke behandlingsaktiviteter kan forbedres. De dataansvarlige skal udvise velvilje til at følge disse henstillinger og underrette PIPC om resultaterne. Når der er rimelig grund til at antage, at der er sket en overtrædelse af PIPA, og det er sandsynligt, at en undladelse af at handle vil forårsage skade, der er vanskelig at rette op, kan PIPC pålægge korrigerende foranstaltninger (artikel 64, stk. 1, i PIPA) ([149]). I afsnit 5 i meddelelse nr. 2021-5 (bilag I) præciseres det med bindende virkning, at disse betingelser er opfyldt med hensyn til overtrædelse af enhver PIPA-bestemmelse, der beskytter den enkeltes ret til privatlivets fred med hensyn til personoplysninger ([150]). De foranstaltninger, som PIPC har beføjelse til at træffe, omfatter påbud om ophør af den adfærd, der forårsager overtrædelsen, midlertidig suspension af databehandlingen eller andre nødvendige foranstaltninger. Manglende overholdelse af en korrigerende foranstaltning kan føre til en sanktion i form af en bøde på højst 50 mio. WON (artikel 75, stk. 2, nr. 13, i PIPA).

(121) Med hensyn til visse offentlige myndigheder (f.eks. nationalforsamlingen, centrale forvaltningsorganer, lokale myndigheder og domstolene) fastsættes det i artikel 64, stk. 4, i PIPA, at PIPC kan »henstille« iværksættelsen af de korrigerende foranstaltninger, der er nævnt i betragtning 120, og at disse myndigheder skal følge sådanne henstillinger, medmindre der foreligger ekstraordinære omstændigheder. Ifølge afsnit 5 i meddelelse nr. 2021-5 forstås herved ekstraordinære faktiske eller retlige omstændigheder, som PIPC ikke var bekendt med, da henstillingen blev fremsat. Den pågældende offentlige myndighed kan kun påberåbe sig sådanne ekstraordinære omstændigheder, hvis den klart påviser, at der ikke er sket en overtrædelse, og PIPC fastslår, at dette rent faktisk ikke er tilfældet. I modsat fald skal den offentlige myndighed følge PIPC's henstilling og »iværksætte en korrigerende foranstaltning, herunder straks bringe handlingen til ophør, og yde skadeserstatning i de ekstraordinære tilfælde, hvor der ikke desto mindre blev begået en ulovlig handling.«

(122) PIPC kan også anmode andre forvaltningsorganer med særlig kompetence i henhold til sektorspecifik lovgivning (f. eks. inden for sundhed og uddannelse) om at foretage en undersøgelse — på egen hånd eller sammen med PIPC — af (formodede) krænkelser af privatlivets fred begået af dataansvarlige, der opererer i disse sektorer under deres kontrol, og om at pålægge korrigerende foranstaltninger (artikel 63, stk. 4-5, i PIPA). I så fald fastlægger PIPC grundlaget og genstanden for og omfanget af undersøgelsen ([151]). Det relevante forvaltningsorgan skal herefter forelægge en inspektionsplan for PIPC og underrette PIPC om resultatet af inspektionen. PIPC kan henstille, at der træffes en specifik korrigerende foranstaltning, som det pågældende organ skal bestræbe sig på at gennemføre. En sådan anmodning begrænser under alle omstændigheder ikke PIPC's kompetence til selv at foretage undersøgelser eller pålægge sanktioner.

([148]) PIPC kan desuden få adgang til den dataansvarliges lokaler for at kontrollere status for forretningsaktiviteter, fortegnelser, dokumenter mv. (artikel 63, stk. 2, i PIPA). Se også artikel 45-3 i CIA og artikel 36-4 i CIA-gennemførelsesdekretet vedrørende PIPC's beføjelser i henhold til denne lov.

([149]) Se også artikel 45-4 i CIA vedrørende PIPC's beføjelser i henhold til CIA.

([150]) Ifølge afsnit 5 i meddelelsen forstås ved »vægtige grunde til at antage, at der er sket en overtrædelse i forbindelse med personoplysninger, og at en undladelse af at handle sandsynligvis vil forårsage skade, der er vanskelig at afhjælpe«, jf. artikel 64, stk. 1 og 2, i PIPA, en overtrædelse af de principper, rettigheder og forpligtelser, der er fastsat i loven for at beskytte den enkeltes ret til personoplysninger. Det samme gælder PIPC's beføjelser i henhold til artikel 45-4 i CIA.

([151]) Artikel 60 i PIPA-gennemførelsesdekretet.

(123) Ud over sine korrigerende beføjelser kan PIPC pålægge administrative bøder på mellem 10 og 50 mio. WON for overtrædelser af forskellige PIPA-krav (artikel 75 i PIPA) ([152]). Dette omfatter bl.a. manglende overholdelse af kravene om lovlig behandling, undladelse af at træffe de nødvendige sikkerhedsforanstaltninger, manglende underretning af registrerede i tilfælde af et brud på datasikkerheden, manglende overholdelse af kravene vedrørende outsourcet behandling, manglende fastlæggelse og offentliggørelse af en politik for beskyttelse af privatlivets fred, undladelse af at udpege en databeskyttelsesansvarlig eller undladelse af at efterkomme en anmodning fra den registrerede under udøvelsen af vedkommendes individuelle rettigheder samt visse proceduremæssige overtrædelser (manglende samarbejde i forbindelse med en undersøgelse). Hvis den samme dataansvarlige overtræder flere bestemmelser i PIPA, kan der pålægges en bøde for hver overtrædelse, og antallet af berørte personer vil blive taget i betragtning ved fastsættelsen af bødens størrelse.

(124) Hvis der er rimelig grund til mistanke om en overtrædelse af PIPA eller andre »databeskyttelseslove«, kan PIPC desuden indgive en anmeldelse til den kompetente efterforskningsmyndighed (f.eks. en anklager, jf. artikel 65, stk. 1, i PIPA). PIPC kan desuden henstille, at den dataansvarlige træffer disciplinære foranstaltninger over for den ansvarlige person (herunder den ansvarlige leder, jf. artikel 65, stk. 2, i PIPA). Efter modtagelsen af denne henstilling skal den dataansvarlige følge ([153]) henstillingen og skriftligt underrette PIPC om resultatet (artikel 65 i PIPA sammenholdt med artikel 58 i PIPA-gennemførelsesdekretet).

(125) Hvad angår henstillinger i henhold til artikel 61, korrigerende foranstaltninger i henhold til artikel 64, anmeldelse eller henstillinger om disciplinære foranstaltninger i henhold til artikel 65 og pålæggelse af administrative bøder i henhold til artikel 75 i PIPA, kan PIPC offentliggøre oplysninger om de faktiske omstændigheder — dvs. om overtrædelsen, den enhed, der har overtrådt loven, og de pålagte foranstaltninger — på sit websted eller i et generelt landsdækkende dagblad (artikel 66 i PIPA sammenholdt med artikel 61, stk. 1, i PIPA-gennemførelsesdekretet) ([154]).

(126) Endelig understøttes overholdelsen af databeskyttelseskravene i PIPA (samt andre »databeskyttelseslove«) af en ordning med strafferetlige sanktioner. I denne forbindelse indeholder artikel 70-73 i PIPA sanktionsbestemmelser, der kan føre til pålæggelse af en bøde (på mellem 20 og 100 mio. WON) eller fængsel (med en maksimumsstraf på mellem 2 og 10 år). Relevante overtrædelser omfatter bl.a. anvendelse af personoplysninger eller videregivelse af sådanne oplysninger til tredjemand uden det nødvendige samtykke, behandling af følsomme oplysninger i strid med forbuddet i artikel 23, stk. 1, i PIPA, manglende overholdelse af gældende sikkerhedskrav, der medfører, at personoplysningerne går tabt, stjæles, videregives, forfalskes, ændres eller beskadiges, undladelse af at træffe de nødvendige foranstaltninger til at berigtige, slette eller suspendere behandlingen af personoplysninger eller ulovlig overførsel af personoplysninger til et tredjeland ([155]). I henhold til artikel 74 i PIPA er den dataansvarliges ansatte, agent eller repræsentant samt den dataansvarlige selv ansvarlig i hvert af disse tilfælde ([156]).

(127) Ud over de strafferetlige sanktioner, der er fastsat i PIPA, kan misbrug af personoplysninger også udgøre en strafbar handling i henhold til straffeloven. Dette er navnlig tilfældet i forbindelse med overtrædelsen af brevhemmeligheden og hemmeligholdelsen af dokumenter eller elektroniske fortegnelser (artikel 316), videregivelse af oplysninger, der er omfattet af tavshedspligt (artikel 317), computersvig (artikel 347-2) samt underslæb og tillidsbrud (artikel 355).

(128) Det koreanske system kombinerer derfor forskellige typer sanktioner, lige fra korrigerende foranstaltninger og administrative bøder til strafferetlige sanktioner, som sandsynligvis vil have en betydelig afskrækkende virkning på dataansvarlige og de personer, der håndterer oplysningerne. Umiddelbart efter oprettelsen i 2020 begyndte PIPC at gøre brug af sine beføjelser. Ifølge PIPC's årsrapport for 2021 har PIPC allerede udstedt en række henstillinger,

([152]) Hvis den dataansvarliges systemer til behandling og beskyttelse af personoplysninger er blevet certificeret som værende i overensstemmelse med PIPA, men certificeringskriterierne i henhold til artikel 34-2, stk. 1, i PIPA-gennemførelsesdekretet rent faktisk ikke er opfyldt, eller i tilfælde af en alvorlig overtrædelse af enhver »lov om beskyttelse af [person]oplysninger«, kan PIPC tilbagekalde certificeringen (artikel 32-2, stk. 3 og 5, i PIPA). PIPC underretter den dataansvarlige om en sådan tilbagekaldelse og bekendtgør eller offentliggør den på sit websted eller i statstidende (artikel 34-4 i PIPA-gennemførelsesdekretet). Der er også fastsat administrative bøder (artikel 52 i CIA) og strafferetlige sanktioner (artikel 50 i CIA) for overtrædelser af CIA.

([153]) I henhold til artikel 58, stk. 2, i PIPA-gennemførelsesdekretet skal den dataansvarlige, hvis særlige omstændigheder gør det »praktisk umuligt« at følge henstillingen, give PIPC en behørig begrundelse.

([154]) Ved beslutningen om denne offentliggørelse skal PIPC tage hensyn til overtrædelsens indhold og alvor, dens varighed og hyppighed samt dens konsekvenser (skadens omfang). Den berørte enhed skal underrettes på forhånd og have mulighed for at forsvare sig, jf. artikel 61, stk. 2 og 3, i PIPA-gennemførelsesdekretet.

([155]) Jf. artikel 71, nr. 2, sammenholdt med artikel 18, stk. 1, i PIPA (manglende overholdelse af betingelserne i artikel 17, stk. 3, i PIPA, som artikel 18, stk. 1, henviser til). Se også artikel 75, stk. 2, nr. 1, sammenholdt med artikel 17, stk. 2, i PIPA (undladelse af at give den berørte person de nødvendige oplysninger i henhold til artikel 17, stk. 2, i PIPA, som artikel 17, stk. 3, henviser til).

([156]) Desuden giver artikel 74-2 i PIPA mulighed for at konfiskere penge, varer eller andre indtægter erhvervet som følge af overtrædelsen, eller, hvis konfiskation er umulig, »at inddrive« den ulovligt opnåede fordel.

administrative bøder og korrigerende foranstaltninger, både til den offentlige sektor (ca. 34 offentlige myndigheder) og private operatører (ca. 140 virksomheder) ([157]). Bemærkelsesværdige sager omfatter f.eks. pålæggelsen af en bøde på 6,7 mia. WON i december 2020 i forbindelse med en virksomhed, der havde overtrådt forskellige bestemmelser i PIPA (herunder sikkerhedskrav, krav om samtykke til videregivelse til tredjemand og gennemsigtighed) ([158]), og pålæggelsen af en bøde på 103,3 mio. WON i april 2021 i forbindelse med en AI-teknologivirksomhed, der bl.a. havde overtrådt reglerne om lovlig behandling, navnlig samtykke, og behandling af pseudonymiserede oplysninger ([159]). I august 2021 afsluttede PIPC endnu en undersøgelse af tre virksomheders aktiviteter, som førte til korrigerende foranstaltninger og pålæggelse af bøder på op til 6,47 mia. WON (bl.a. for manglende underretning af enkeltpersoner om videregivelsen af personoplysninger til tredjemand, herunder overførsler til tredjelande) ([160]). Allerede inden den nylige reform havde Sydkorea også gode håndhævelsesresultater, og de ansvarlige myndigheder gjorde brug af hele spektret af håndhævelsesforanstaltninger, herunder administrative bøder, korrigerende foranstaltninger og navngivning af en række dataansvarlige, herunder udbydere af kommunikationstjenester (Koreas kommunikationskommission) samt kommercielle operatører, finansielle institutioner, offentlige myndigheder, universiteter og hospitaler (indenrigs- og sikkerhedsministeriet) ([161]). På dette grundlag konkluderer Kommissionen, at det koreanske system sikrer en effektiv håndhævelse af databeskyttelsesreglerne i praksis og dermed sikrer et beskyttelsesniveau, som i det væsentlige svarer til det niveau, der er fastsat i forordning (EU) 2016/679.

2.5. **Klageadgang**

(129) Med henblik på at sikre tilstrækkelig beskyttelse og navnlig håndhævelse af individuelle rettigheder bør den registrerede have effektive muligheder for administrativ og retslig prøvelse, herunder mulighed for at opnå skadeserstatning.

(130) Det koreanske system giver enkeltpersoner adgang til forskellige effektive mekanismer til at håndhæve deres rettigheder og få adgang til (retslig) prøvelse.

(131) Som et første skridt kan personer, der mener, at deres databeskyttelsesrettigheder eller -interesser er blevet krænket, henvende sig til den relevante dataansvarlige. I henhold til artikel 30, stk. 1, nr. 5, i PIPA skal den dataansvarliges politik for beskyttelse af privatlivets fred bl.a. indeholde oplysninger om de registreredes rettigheder og om, hvordan de udøves. Den skal desuden indeholde kontaktoplysninger — såsom navn og telefonnummer på den databeskyttelsesansvarlige eller den afdeling, der er ansvarlig for databeskyttelse — for at gøre det muligt at indgive klager). I den dataansvarliges organisation har den databeskyttelsesansvarlige til opgave at behandle klager, træffe korrigerende foranstaltninger i tilfælde af krænkelse af privatlivets fred og afhjælpende foranstaltninger (artikel 31, stk. 2, nr. 3, og artikel 31, stk. 4, i PIPA). Sidstnævnte er f.eks. relevant i tilfælde af et brud på datasikkerheden, da den dataansvarlige skal underrette den registrerede om kontaktpunktet eller -punkterne for bl.a. indberetning af skade (artikel 34, stk. 1, nr. 5, i PIPA).

(132) Desuden har enkeltpersoner i henhold til PIPA adgang til en række muligheder for at få prøvet deres sag mod dataansvarlige. For det første kan enhver, der mener, at vedkommendes databeskyttelsesrettigheder eller -interesser er blevet krænket af den dataansvarlige, indberette en sådan overtrædelse direkte til PIPC og/eller en af de specialiserede institutioner, som PIPC har udpeget til at modtage og behandle klager, herunder Koreas internet- og sikkerhedsagentur, som til dette formål driver et callcenter for personoplysninger (det såkaldte »callcenter for privatlivsbeskyttelse«) (artikel 62, stk. 1 og 2, i PIPA sammenholdt med artikel 59 i PIPA-gennemførelsesdekretet). Callcentret for privatlivsbeskyttelse undersøger og fastslår overtrædelser, yder rådgivning i forbindelse med behandling af personoplysninger (artikel 62, stk. 3, i PIPA) og kan indberette overtrædelser til PIPC (men kan

([157]) Se PIPC's årsrapport for 2021, s. 50-55 (kun tilgængelig på koreansk), på https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7511#LINK.

([158]) Se (kun tilgængelig på koreansk) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=6954#LINK.

([159]) Se (kun tilgængelig på koreansk) https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7298&fbclid=IwAR3SKcMQi6G5pR9k4I7j6GNXtc8aBVDOwcURevvvzQtYI7AS40UKYXoOXo8.

([160]) Se (kun tilgængelig på koreansk): https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=7497#LINK.

([161]) Jf. f.eks. årsrapporten for 2020 på (kun på koreansk) https://www.pipc.go.kr/np/cop/bbs/selectBoardList.do?bbsId=BS079&mCode=D070020000 og eksemplerne på engelsk på https://www.privacy.go.kr/eng/enforcement_02.do.

ikke selv træffe håndhævelsesforanstaltninger). Callcentret for privatlivsbeskyttelse modtager et stort antal klager/anmodninger (f.eks. 177 457 i 2020, 159 255 i 2019 og 164 497 i 2018) ([162]). Ifølge oplysninger fra PIPC modtog PIPC selv ca. 1 000 klager mellem august 2020 og august 2021. Som svar på en klage kan PIPC fremsætte henstillinger om forbedringer og korrigerende foranstaltninger, indgive en »anmeldelse« til den kompetente undersøgelsesmyndighed (herunder en anklager) eller fremsætte henstillinger om disciplinære foranstaltninger (jf. artikel 61, 64 og 65 i PIPA). PIPC's afgørelser (f.eks. afslag på at behandle en klage eller afslag på en klage) kan anfægtes i medfør af lov om forvaltningssager ([163]).

(133) For det andet kan registrerede i henhold til artikel 40-50 i PIPA sammenholdt med artikel 48-14 til 57 i PIPA-gennemførelsesdekretet indgive en klage til tvistbilæggelsesudvalget, som består af repræsentanter, der udpeges af formanden for PIPC blandt medlemmerne af PIPC's øverste ledelse, og af enkeltpersoner, der udpeges på grundlag af deres erfaring inden for databeskyttelse blandt bestemte grupper (jf. artikel 40, stk. 2, 3 og 7, i PIPA og artikel 48-14 i PIPA-gennemførelsesdekretet) ([164]). Muligheden for at gøre brug af mægling i tvistbilæggelsesudvalget er en alternativ klageadgang, men begrænser ikke den enkeltes ret til at klage til PIPC eller gå til domstolene. I forbindelse med behandlingen af sagen kan udvalget anmode tvistens parter om at udlevere det nødvendige materiale og/eller indkalde relevante vidner til at give møde for udvalget (artikel 45 i PIPA). Når sagen er afklaret, udarbejder udvalget et mæglingsforslag ([165]), som skal støttes af et flertal blandt medlemmerne. Mæglingsforslaget kan omfatte krav om, at overtrædelsen bringes til ophør, nødvendige afhjælpende foranstaltninger (herunder genopretning eller erstatning) samt nødvendige foranstaltninger til at forhindre, at de samme eller lignende overtrædelser gentager sig (artikel 47, stk. 1, i PIPA). Hvis begge parter accepterer mæglingskendelsen, vil den have samme virkning som et retsforlig (artikel 47, stk. 5, i PIPA). Begge parter kan anlægge en retssag under mæglingen, og i så fald suspenderes sidstnævnte (jf. artikel 48, stk. 2, i PIPA) ([166]). De årlige tal fra PIPC viser, at enkeltpersoner regelmæssigt gør brug af proceduren ved tvistbilæggelsesudvalget, hvilket ofte fører til et vellykket resultat. I 2020 behandlede udvalget f.eks. 126 sager, hvoraf 89 blev afgjort i udvalget (i 77 af sagerne nåede parterne allerede til enighed, inden mæglingsprocessens afslutning, og i 12 sager accepterede parterne mæglingsforslaget), hvilket førte til en mæglingsprocent på 70,6 % ([167]). I 2019 behandlede udvalget 139 sager, hvoraf 92 blev afgjort, hvilket førte til en mæglingsprocent på 62,2 %.

(134) Hvis mindst 50 personer lider skade, eller hvis deres databeskyttelsesrettigheder er blevet krænket på samme eller lignende måde som følge af den samme (type) hændelse ([168]), kan en registreret eller en databeskyttelsesorganisation ansøge om kollektiv tvistbilæggelse på vegne af denne gruppe. Andre registrerede kan ansøge om at deltage i en sådan mægling, som bekendtgøres offentligt af tvistbilæggelsesudvalget (artikel 49, stk. 1-3, i PIPA sammenholdt med artikel 52-54 i PIPA-gennemførelsesdekretet) ([169]). Tvistbilæggelsesudvalget kan vælge mindst én

([162]) Jf. PIPC's årsrapport for 2021, s. 174. I 2020 vedrørte sådanne klager f.eks. indsamling af oplysninger uden samtykke, manglende overholdelse af gennemsigtighedsforpligtelser, databehandleres overtrædelser af PIPA, utilstrækkelige sikkerhedsforanstaltninger, manglende svar på anmodninger fra registrerede samt generelle forespørgsler.

([163]) Enkeltpersoner kan navnlig påklage et forvaltningsorgans udøvelse af eller afvisning af at udøve offentlig myndighed (artikel 2, stk. 1, nr. 1, og artikel 3, nr. 1, i lov om forvaltningssager). Der er mere detaljerede oplysninger om proceduremæssige aspekter, herunder krav til antagelighed, i betragtning 181.

([164]) Alle medlemmerne har en fast mandatperiode og kan kun afsættes, hvis det er berettiget (jf. artikel 40, stk. 5, og artikel 41 i PIPA). Artikel 42 i PIPA indeholder desuden garantier til beskyttelse mod interessekonflikter.

([165]) Jf. artikel 44 i PIPA. Derudover kan udvalget foreslå et udkast til forlig og anbefale forlig uden mægling (jf. artikel 46 i PIPA).

([166]) Udvalget kan desuden afvise mægling, hvis det finder det uhensigtsmæssigt at mægle i tvisten i betragtning af dens karakter, eller fordi anmodningen om mægling blev indgivet med et urimeligt formål (artikel 48 i PIPA).

([167]) Jf. PIPC's årsrapport for 2021, s. 179. Disse sager vedrørte bl.a. overtrædelser af kravet om samtykke til indsamling af oplysninger, princippet om formålsbegrænsning og de registreredes rettigheder.

([168]) Jf. artikel 49, stk. 1, i PIPA, ifølge hvilken de registrerede skal lide skade eller se deres rettigheder krænket »på samme eller lignende måde«, og artikel 52, nr. 2, i PIPA-gennemførelsesdekretet, som gør det til en betingelse, at »vigtige aspekter af hændelsen er faktisk eller retligt de samme«.

([169]) Desuden kan tredjeparter også drage fordel af en kollektiv mæglingskendelse, der accepteres af den dataansvarlige, da tvistbilæggelsesudvalget kan anmode den dataansvarlige om at udarbejde og forelægge en erstatningsplan, som (også) omfatter dem (artikel 49, stk. 5, i PIPA).

person, der bedst varetager den fælles interesse som en repræsentativ part (artikel 49, stk. 4, i PIPA). Hvis den dataansvarlige afviser kollektiv tvistbilæggelse eller ikke accepterer mæglingsforslaget, kan visse organisationer ([170]) anlægge et kollektivt søgsmål for at imødegå overtrædelsen (artikel 51-57 i PIPA).

(135) For det tredje har den registrerede i tilfælde af en krænkelse af privatlivets fred, der forvolder »skade« på den registrerede, ret til passende erstatning gennem en »hurtig og retfærdig procedure« (artikel 4, nr. 5, sammenholdt med artikel 39 i PIPA) ([171]). Den dataansvarlige kan bevise sin uskyld ved at påvise, at vedkommende ikke har begået nogen fejl (»forsæt eller forsømmelighed«). Hvis den registrerede lider skade som følge af tab, tyveri, videregivelse, forfalskning, ændring eller beskadigelse af den registreredes personoplysninger, kan retten fastsætte en erstatning på op til tre gange den faktiske skade under hensyntagen til en række faktorer (artikel 39, stk. 3 og 4, i PIPA). Alternativt kan den registrerede kræve en »rimelig erstatning« på højst 3 mio. WON (artikel 39-2, stk. 1 og 2, i PIPA). I henhold til civilloven kan der desuden kræves erstatning fra enhver, »der forvolder tab eller påfører en anden person skade som følge af en ulovlig handling begået forsætligt eller uagtsomt« ([172]), eller fra en person, »som har skadet en anden person eller dennes frihed eller omdømme, eller som har påført en anden person psykisk angst« ([173]). Et sådant ansvar uden for kontraktforhold som følge af overtrædelse af databeskyttelsesreglerne er blevet bekræftet af højesteret ([174]). Hvis der er forvoldt skade som følge af en offentlig myndigheds ulovlige handling, kan der desuden indgives et erstatningskrav i medfør af lov om erstatning fra staten ([175]). Et krav i henhold til lov om erstatning fra staten kan indgives til et specialiseret »erstatningsråd« eller direkte til de koreanske domstole ([176]). Statens erstatningsansvar omfatter også immaterielle skader (f.eks. psykiske lidelser) ([177]). Hvis offeret er udenlandsk statsborger, finder lov om erstatning fra staten anvendelse, hvis vedkommendes hjemland ligeledes sikrer koreanske statsborgere erstatning fra staten ([178]).

(136) For det fjerde har højesteret anerkendt, at enkeltpersoner har ret til at anmode om nedlæggelse af et forbud eller påbud i forbindelse med krænkelser af deres rettigheder i henhold til forfatningen, herunder retten til beskyttelse af personoplysninger ([179]). I denne forbindelse kan en domstol f.eks. pålægge dataansvarlige at suspendere eller standse enhver ulovlig aktivitet. Derudover kan databeskyttelsesrettigheder, herunder de rettigheder, der er beskyttet af PIPA, håndhæves via civile søgsmål. Højesteret har anerkendt denne horisontale anvendelse af den forfatningsmæssige beskyttelse af privatlivets fred på forholdet mellem private parter ([180]).

([170]) Forbrugergrupper eller nonprofit-NGO'er med et vist antal medlemmer, hvis erklærede formål er databeskyttelse (for nonprofit-NGO'er kræves det desuden, at mindst 100 registrerede, der har oplevet samme (type) overtrædelse, har indgivet en anmodning om at anlægge et kollektivt søgsmål). Jf. artikel 51 i PIPA.

([171]) Artikel 43 til 43-3 i CIA fastsætter også et erstatningsansvar for skader som følge af overtrædelser af denne lov.

([172]) Artikel 750 i civilloven.

([173]) Artikel 751, stk. 1, i civilloven.

([174]) Jf. f.eks. højesterets afgørelser 2015Da251539, 251546, 251553, 251560 og 251577 af 30. maj 2018. Højesteret bekræftede desuden, at brud på datasikkerheden kan føre til tilkendelse af erstatning i henhold til civilloven, jf. højesterets afgørelser 2011Da59834, 59858 og 59841 af 26. december 2012 (engelsk resumé findes på http://library.scourt.go.kr/SCLIB_data/decision/9-69%202012.12.26.2011Da59834.htm). I denne sag præciserede højesteret, at der for at vurdere, om en person har lidt psykisk overlast, der kan betegnes som en erstatningspligtig skade, bør tages hensyn til en række faktorer såsom typen og karakteren af de lækkede oplysninger, identificerbarheden af den pågældende person som følge af bruddet, tredjemands mulighed for at få adgang til oplysningerne, i hvilket omfang personoplysningerne blev spredt, om dette førte til yderligere krænkelser af individuelle rettigheder, hvordan personoplysningerne blev forvaltet og beskyttet mv.

([175]) På grundlag af lov om erstatning fra staten kan personer søge erstatning for skade, som offentligt ansatte har forvoldt under udøvelsen af deres officielle hverv i strid med loven (lovens artikel 2, stk. 1).

([176]) Artikel 9 og 12 i lov om erstatning fra staten. Ved loven oprettes distriktsråd (under forsæde af vicestatsadvokaten ved den tilsvarende anklagemyndighed), et centralråd (under forsæde af vicejustitsministeren) og et særligt råd (med ansvar for erstatningskrav for skade forvoldt af militærpersonel eller civilansatte i militæret under forsæde af viceforsvarsministeren). Erstatningskrav behandles i princippet af distriktsråd, som under visse omstændigheder skal videresende sagerne til det centrale/særlige råd, f.eks. hvis erstatningen overstiger et vist beløb, eller hvis en person anmoder om fornyet behandling. Alle råd består af medlemmer udpeget af justitsministeren (f.eks. blandt embedsmænd i justitsministeriet, retsembedsmænd, advokater og personer med ekspertise inden for erstatning fra staten) og er underlagt specifikke regler om interessekonflikter (jf. artikel 7 i gennemførelsesdekretet til lov om erstatning fra staten).

([177]) Jf. artikel 8 i lov om erstatning fra staten (hvor der henvises til civilloven) og artikel 751 i civilloven.

([178]) Artikel 7 i lov om erstatning fra staten.

([179]) Højesterets afgørelse 93Da40614 af 12. april 1996 og afgørelse 2008Da42430 af 2. september 2011 (engelsk resumé findes på https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

([180]) Jf. f.eks. højesterets afgørelse 2008Da42430 af 2. september 2011 (engelsk resumé findes på https://www.scourt.go.kr/eng/supreme/decisions/NewDecisionsView.work?seq=696&pageIndex=1&mode=6&searchWord=).

(137) Endelig kan enkeltpersoner indgive en anmeldelse i henhold til strafferetsplejeloven (artikel 223) til en offentlig anklager eller kriminalpolitiet ([181]).

(138) I det koreanske system er der derfor forskellige klagemuligheder, lige fra let tilgængelige og billige muligheder (f.eks. ved at kontakte callcentret for privatlivsbeskyttelse eller gennem (kollektiv) mægling) til administrative klagemuligheder (via PIPC) og retlige klagemuligheder, herunder mulighed for at opnå skadeserstatning.

3. KOREANSKE OFFENTLIGE MYNDIGHEDERS ADGANG TIL OG ANVENDELSE AF PERSONOPLYSNINGER OVERFØRT FRA DEN EUROPÆISKE UNION

(139) Kommissionen har også vurderet begrænsningerne og garantierne, herunder tilsynet og de enkelte prøvelsesmekanismer i koreansk ret, i forbindelse med koreanske offentlige myndigheders indsamling og efterfølgende anvendelse af personoplysninger, der er blevet overført til dataansvarlige i Korea i offentlighedens interesse, navnlig med henblik på strafferetlig håndhævelse og til nationale sikkerhedsformål (myndighedsadgang). I den forbindelse har Kommissionen modtaget officielle redegørelser, forsikringer og tilsagn fra Korea undertegnet på højeste ministerielle og forvaltningsmæssige niveau, og disse findes i bilag II til denne afgørelse.

(140) Ved vurderingen af, om de betingelser, hvorunder myndighedsadgangen til oplysninger, der overføres til Korea i medfør af denne afgørelse, opfylder væsentlighedskriteriet i henhold til artikel 45, stk. 1, i forordning (EU) 2016/679, som fortolket af Den Europæiske Unions Domstol i lyset af chartret om grundlæggende rettigheder, har Kommissionen navnlig taget hensyn til følgende kriterier.

(141) For det første skal enhver begrænsning af retten til beskyttelse af personoplysninger være fastsat ved lov, og det retsgrundlag, der gør det muligt at gribe ind i en sådan ret, skal selv fastlægge omfanget af begrænsningen af udøvelsen af den pågældende rettighed ([182]).

(142) For at opfylde kravet om proportionalitet, som indebærer, at undtagelser fra og begrænsninger af beskyttelsen af personoplysninger kun finder anvendelse i det omfang, det er strengt nødvendigt i et demokratisk samfund for at opfylde specifikke mål af almen interesse svarende til dem, der er anerkendt af Unionen, skal den lovgivning i det pågældende tredjeland, der tillader dette indgreb, for det andet fastsætte klare og præcise regler for omfanget og anvendelsen af de pågældende foranstaltninger og minimumsgarantier, således at de personer, hvis oplysninger er blevet videregivet, har tilstrækkelige garantier til effektivt at beskytte deres personoplysninger mod risikoen for misbrug ([183]). Lovgivningen skal navnlig angive, under hvilke omstændigheder og på hvilke betingelser der kan vedtages en foranstaltning om behandling af sådanne oplysninger ([184]). Desuden skal den sikre et uafhængigt tilsyn med, at disse krav opfyldes ([185]).

(143) For det tredje skal denne lovgivning og dens krav være retligt bindende i henhold til national ret. Dette vedrører først og fremmest myndighederne i det pågældende tredjeland, men disse retlige krav skal også kunne håndhæves ved domstolene over for disse myndigheder ([186]). De registrerede skal navnlig have mulighed for at anlægge sag ved en uafhængig og upartisk domstol for at få adgang til deres personoplysninger eller for at få sådanne oplysninger berigtiget eller slettet ([187]).

3.1. **Den overordnede retlige ramme**

(144) De begrænsninger og garantier, der gælder for de koreanske offentlige myndigheders indsamling og efterfølgende anvendelse af personoplysninger, følger af de overordnede forfatningsmæssige rammer, specifikke love, der regulerer deres aktiviteter inden for strafferetlig håndhævelse og national sikkerhed, samt de specifikke regler for behandling af personoplysninger.

([181]) Som forklaret i betragtning 127 kan misbrug af oplysninger udgøre en strafbar handling i henhold til straffeloven.
([182]) Jf. Schrems II, præmis 174-175 og den nævnte retspraksis. Se også sag C-623/17 Privacy International ECLI:EU:C:2020:790, præmis 65, for så vidt angår adgang for medlemsstaternes offentlige myndigheder, og forenede sager C-511/18, C-512/18 og C-520/18, La Quadrature du Net m.fl., ECLI:EU:C:2020:791, præmis 175.
([183]) Jf. Schrems II, præmis 176 og 181, og den nævnte retspraksis. Se også Privacy International, præmis 68, for så vidt angår adgang for offentlige myndigheder i medlemsstaterne, og La Quadrature du Net m.fl., præmis 132.
([184]) Jf. Schrems II, præmis 176. Se også Privacy International, præmis 68, for så vidt angår adgang for offentlige myndigheder i medlemsstaterne, og La Quadrature du Net m.fl., præmis 132.
([185]) Jf. Schrems II, præmis 179.
([186]) Jf. Schrems II, præmis 181-182.
([187]) Jf. Schrems I, præmis 95, og Schrems II, præmis 194. I den forbindelse har EU-Domstolen navnlig understreget, at overholdelsen af artikel 47 i chartret om grundlæggende rettigheder, der garanterer retten til effektive retsmidler ved en uafhængig og upartisk domstol, »bidrager til det krævede beskyttelsesniveau i Den Europæiske Union […], som Kommissionen skal fastslå er overholdt, før den vedtager en afgørelse om tilstrækkeligheden af beskyttelsesniveauet i henhold til databeskyttelsesforordningens artikel 45, stk. 1«, i forordning (EU) 2016/679 (Schrems II, præmis 186).

(145) For det første er de koreanske offentlige myndigheders adgang til personoplysninger underlagt de generelle principper om lovlighed, nødvendighed og proportionalitet, der følger af den koreanske forfatning ([188]). Grundlæggende rettigheder og friheder (herunder retten til privatlivets fred og retten til privatlivets fred i forbindelse med korrespondance) ([189]) må navnlig kun begrænses ved lov, og når det er nødvendigt af hensyn til den nationale sikkerhed eller opretholdelsen af lov og orden og den offentlige velfærd. Sådanne begrænsninger må ikke berøre den pågældende rettigheds eller friheds væsentlige indhold. Med hensyn til ransagninger og beslaglæggelser fastsættes det specifikt i forfatningen, at de kun kan finde sted i henhold til loven på grundlag af en retskendelse og under overholdelse af princippet om en retfærdig rettergang ([190]). Endelig kan enkeltpersoner påberåbe sig deres rettigheder og friheder ved forfatningsdomstolen, hvis de mener, at de er blevet krænket af offentlige myndigheder under udøvelsen af deres beføjelser ([191]). Personer, der har lidt skade som følge af en ulovlig handling begået af offentligt ansatte under udøvelsen af deres officielle hverv, har ligeledes ret til at kræve en rimelig erstatning ([192]).

(146) For det andet afspejles de generelle principper i betragtning 145 som nærmere beskrevet i afsnit 3.2.1 og 3.3.1 også i de specifikke love, der regulerer de retshåndhævende myndigheders og nationale sikkerhedsmyndigheders beføjelser. Med hensyn til strafferetlige efterforskninger fastsættes det f.eks. i strafferetsplejeloven (CPA), at der kun må træffes obligatoriske foranstaltninger, hvis det er udtrykkeligt fastsat i CPA, og i det mindst mulige omfang for at nå formålet med efterforskningen ([193]). På samme måde forbyder artikel 3 i lov om beskyttelse af privatlivets fred i forbindelse med kommunikation (CPPA) adgang til privat kommunikation, undtagen på grundlag af loven og med forbehold af de begrænsninger og garantier, der er fastsat heri. På det nationale sikkerhedsområde fastsættes det i lov om den nationale efterretningstjeneste (NIS-loven), at enhver adgang til kommunikation eller lokaliseringsdata skal være i overensstemmelse med loven, og misbrug af beføjelser og overtrædelser af loven omfattes af strafferetlige sanktioner ([194]).

(147) For det tredje er offentlige myndigheders behandling af personoplysninger, herunder med henblik på retshåndhævelse og til nationale sikkerhedsformål, omfattet af databeskyttelsesreglerne i PIPA ([195]). Som et generelt princip pålægger artikel 5, stk. 1, i PIPA offentlige myndigheder at formulere politikker til forebyggelse af »misbrug og forkert anvendelse af personoplysninger, indiskret overvågning og sporing mv. og styrkelse af den enkeltes værdighed og ret til privatlivets fred«. Endvidere skal enhver dataansvarlig behandle personoplysninger på en måde, der minimerer risikoen for at krænke den registreredes ret til privatlivets fred (artikel 3, stk. 6, i PIPA).

(148) Alle de PIPA-krav, der er nærmere beskrevet i afsnit 2, gælder for behandling af personoplysninger med henblik på retshåndhævelse. Dette omfatter de centrale principper (såsom lovlighed og rimelighed, formålsbegrænsning, nøjagtighed, dataminimering, opbevaringsbegrænsning, sikkerhed og gennemsigtighed), forpligtelser (f.eks. med hensyn til anmeldelse af brud på datasikkerheden og følsomme oplysninger) og rettigheder (ret til indsigt i og berigtigelse, sletning og suspension).

(149) Behandlingen af personoplysninger til nationale sikkerhedsformål er omfattet af et mere begrænset sæt bestemmelser i PIPA, men de centrale principper samt reglerne om tilsyn, håndhævelse og klage og prøvelsesadgang finder anvendelse ([196]). I artikel 3 og 4 i PIPA fastsættes mere specifikt de generelle databeskyttelsesprincipper (lovlighed og rimelighed, formålsbegrænsning, nøjagtighed, dataminimering, sikkerhed og gennemsigtighed) og individuelle rettigheder (retten til at blive underrettet, retten til indsigt og retten til berigtigelse, sletning og suspension) ([197]). I henhold til artikel 4, stk. 5, i PIPA har registrerede desuden ret til passende erstatning for enhver skade, der opstår som følge af behandlingen af deres personoplysninger, gennem en hurtig og retfærdig

([188]) Jf. bilag II, afsnit 1.1.
([189]) Forfatningens artikel 37, stk. 2.
([190]) Forfatningens artikel 16 og artikel 12, stk. 3. I artikel 12, stk. 3, i forfatningen fastsættes endvidere de ekstraordinære omstændigheder, hvorunder der kan foretages ransagning eller beslaglæggelse (selv om der stadig kræves en efterfølgende kendelse), dvs. i tilfælde af flagrante delicto eller forbrydelser med en fængselsstraf på mindst tre år, hvis der er risiko for, at bevismateriale vil blive ødelagt, eller at den mistænkte undslipper.
([191]) Artikel 68, stk. 1, i lov om forfatningsdomstolen.
([192]) Forfatningens artikel 29, stk. 1.
([193]) Artikel 199, stk. 1, i CPA. Mere generelt skal offentlige myndigheder under udøvelsen af deres beføjelser i henhold til CPA respektere de mistænkte for forbrydelsens og andre berørte personers grundlæggende rettigheder (artikel 198, stk. 2, i CPA).
([194]) Artikel 14 i NIS-loven.
([195]) Jf. bilag II, afsnit 1.2.
([196]) Artikel 58, stk. 1, nr. 2, i PIPA. Se også afsnit 6 i meddelelse nr. 2021-5 (bilag I). Denne undtagelse fra visse bestemmelser i PIPA finder kun anvendelse, når personoplysninger behandles »til nationale sikkerhedsformål«. Når den nationale sikkerhedssituation, der begrunder databehandlingen, er ophørt, kan undtagelsen ikke længere anvendes, og alle PIPA-krav finder anvendelse.
([197]) Sådanne rettigheder kan kun begrænses, når det er fastsat ved lov, i det omfang og så længe det er nødvendigt og forholdsmæssigt for at beskytte et vigtigt mål af samfundsmæssig interesse, eller hvis indrømmelsen af rettigheden kan skade tredjemands liv eller legeme eller er en uberettiget krænkelse af tredjemands ejendom og andre interesser. Jf. afsnit 6 i meddelelse nr. 2021-5.

procedure. Dette suppleres af mere specifikke forpligtelser til kun at behandle personoplysninger i mindst muligt omfang for at nå det tilsigtede formål og ikke længere end nødvendigt, til at træffe de nødvendige foranstaltninger til at garantere en sikker dataforvaltning og korrekt behandling (såsom tekniske, ledelsesmæssige og fysiske garantier) samt til at træffe foranstaltninger til korrekt behandling af individuelle klager ([198]). Endelig finder de generelle principper om lovlighed, nødvendighed og proportionalitet i den koreanske forfatning (jf. betragtning 145) også anvendelse på behandling af personoplysninger til nationale sikkerhedsformål.

(150) Disse generelle begrænsninger og garantier kan påberåbes af enkeltpersoner ved uafhængige tilsynsorganer (f.eks. PIPC og/eller den nationale menneskerettighedskommission, jf. betragtning 177-178), og domstolene (jf. betragtning 179-183) for at få prøvet deres sag.

3.2. **De koreanske myndigheders adgang til og anvendelse af personoplysninger med henblik på strafferetlig håndhævelse**

(151) Republikken Koreas lovgivning pålægger en række begrænsninger af adgangen til og anvendelsen af personoplysninger med henblik på strafferetlig håndhævelse og indeholder en række tilsyns- og prøvelsesmekanismer, som er i overensstemmelse med de krav, der er omhandlet i betragtning 141-143 i denne afgørelse. De betingelser, hvorunder en sådan adgang kan finde sted, og de garantier, der gælder for udøvelsen af disse beføjelser, vurderes nærmere i de følgende afsnit.

3.2.1. *Retsgrundlag, begrænsninger og garantier*

(152) Personoplysninger, der behandles af koreanske dataansvarlige, og som vil blive overført fra Unionen i henhold til denne afgørelse ([199]), kan indsamles af de koreanske myndigheder med henblik på strafferetlig håndhævelse i forbindelse med ransagning eller beslaglæggelse (på grundlag af CPA) via adgang til kommunikationsdata (på grundlag af CPPA) eller indhentning abonnentoplysninger på grundlag af anmodninger om frivillig fremlæggelse af oplysninger (på grundlag af telekommunikationsloven (TBA)) ([200]).

3.2.1.1. Ransagning og beslaglæggelse

(153) I henhold til CPA må ransagning eller beslaglæggelse kun må finde sted, hvis en person mistænkes for en forbrydelse, det er nødvendigt for efterforskningen, og der etableres en forbindelse mellem efterforskningen og den person, der skal ransages, eller den genstand, der skal inspiceres eller beslaglægges ([201]). Desuden må ransagning eller beslaglæggelse (som enhver obligatorisk foranstaltning) kun tillades/foretages i nødvendigt omfang ([202]). Hvis ransagningen vedrører en diskette eller et andet datalagringsmedium, er det i princippet kun de nødvendige oplysninger (i kopi eller udskrevet), der beslaglægges, og ikke hele mediet ([203]). Mediet kan kun beslaglægges, hvis det anses for at være stort set umuligt at udskrive eller kopiere de krævede oplysninger særskilt, eller hvis det anses for at være praktisk umuligt at opfylde formålet med ransagningen på anden vis ([204]). CPA fastsætter derfor klare og præcise regler for omfanget og anvendelsen af disse foranstaltninger, hvorved det sikres, at indgrebet i enkeltpersoners rettigheder i forbindelse med en ransagning eller beslaglæggelse begrænses til, hvad der er nødvendigt for en specifik strafferetlig efterforskning, og står i rimeligt forhold til det forfulgte formål.

([198]) Artikel 58, stk. 4, i PIPA.

([199]) Jf. bilag II, afsnit 2.1. I den koreanske regerings officielle redegørelse (afsnit 2.1 i bilag II) henvises også til muligheden for at indsamle oplysninger om finansielle transaktioner med henblik på at forebygge hvidvaskning af penge og finansiering af terrorisme på grundlag af lov om indberetning og anvendelse af specifikke oplysninger om finansielle transaktioner (ARUSFTI). ARUSFTI pålægger imidlertid kun dataansvarlige, der behandler personlige kreditoplysninger i henhold til CIA, oplysningsforpligtelser, og de er underlagt FSC's tilsyn (jf. betragtning 13). Da sådanne dataansvarliges behandling af personlige kreditoplysninger er udelukket fra denne afgørelses anvendelsesområde, er ARUSFTI ikke relevant for denne vurdering.

([200]) I artikel 3 i CPPA henvises også til lov om militærdomstolen som et muligt retsgrundlag for indsamling af kommunikationsdata. Loven regulerer imidlertid indsamlingen af oplysninger om militærpersonel og kan kun finde anvendelse på civile i et begrænset antal tilfælde (f.eks. hvis militærpersonel og civile begår en forbrydelse sammen, eller hvis en person begår en forbrydelse mod militæret, kan der anlægges sag ved en militærdomstol, jf. artikel 2 i lov om militærdomstolen). Under alle omstændigheder indeholder den generelle bestemmelser om ransagning og beslaglæggelse, der svarer til bestemmelserne i CPA (jf. f.eks. artikel 146-149 og 153-156 i lov om militærdomstolen), og det fastsættes f.eks., at postforsendelser kun må indsamles, når det er nødvendigt for en efterforskning og på grundlag af en kendelse fra militærdomstolen. I det omfang elektronisk kommunikation indsamles på grundlag af denne lov, finder begrænsningerne og garantierne i CPPA anvendelse (jf. bilag II, afsnit 2.2.2., og fodnote 50).

([201]) Artikel 215, stk. 1 og 2, i CPA. Se også artikel 106, stk. 1, og artikel 107 og 109 i CPA, hvori det fastsættes, at domstolene kan foretage ransagning og beslaglæggelse, så længe de pågældende genstande eller personer anses for at være forbundet med en specifik sag. Jf. bilag II, afsnit 2.2.1.2.

([202]) Artikel 199, stk. 1, i CPA.

([203]) Artikel 106, stk. 3, i CPA.

([204]) Artikel 106, stk. 3, i CPA.

(154) Med hensyn til proceduremæssige garantier skal der i henhold til CPA indhentes en retskendelse med henblik på ransagning eller beslaglæggelse ([205]). Ransagning eller beslaglæggelse uden en kendelse er kun undtagelsesvis tilladt, nemlig i hastetilfælde ([206]) på stedet i forbindelse med anholdelsen eller tilbageholdelsen af den mistænkte for forbrydelsen ([207]), eller hvis en genstand bortsmides eller udleveres frivilligt af den mistænkte for forbrydelsen eller tredjemand (for så vidt angår personoplysninger, af den pågældende person selv) ([208]). Ulovlige ransagninger og beslaglæggelser er underlagt strafferetlige sanktioner ([209]), og ethvert bevismateriale, der er indhentet i strid med CPA, betragtes som uantageligt ([210]). Endelig skal de berørte personer altid straks underrettes om en ransagning eller beslaglæggelse (herunder beslaglæggelse af deres oplysninger) ([211]), hvilket vil lette udøvelsen af den enkeltes materielle rettigheder og prøvelsesadgang (om muligheden for at anfægte fuldbyrdelsen af en retskendelse om beslaglæggelse, jf. betragtning 180).

3.2.1.2. Adgang til kommunikationsdata

(155) På grundlag af CPPA kan de koreanske strafferetlige håndhævelsesmyndigheder træffe to typer foranstaltninger ([212]): På den ene side indsamling af »kommunikationsbekræftelsesdata« ([213]), herunder om telekommunikationsdato, start- og sluttidspunkt, antal udgående og indgående opkald samt den anden parts abonnentnummer, hyppighed, logfiler om brugen af teletjenester og lokaliseringsdata (f.eks. fra transmissionstårne, hvor der modtages signaler), og på den anden side »kommunikationsbegrænsende foranstaltninger«, som både omfatter indsamling af indholdet af traditionel post og direkte aflytning af indholdet af telekommunikation ([214]).

(156) Kommunikationsbekræftelsesdata må kun tilgås, når det er nødvendigt for at gennemføre en strafferetlig efterforskning eller fuldbyrde en dom ([215]), på grundlag af en retskendelse ([216]). I denne forbindelse skal der i henhold til CPPA gives detaljerede oplysninger i både anmodningen om kendelsen (f.eks. om begrundelsen for anmodningen, forbindelsen til den pågældende part/abonnenten og de nødvendige oplysninger) og i selve kendelsen (f.eks. om foranstaltningens formål, mål og omfang) ([217]). Indsamling må kun finde sted uden en kendelse, når hensynet til sagens hastende karakter gør det umuligt at indhente en retskendelse, og kendelsen skal i så fald

([205]) Artikel 215, stk. 1 og 2, i CPA, og artikel 113 i CPA. I forbindelse med anmodningen om en kendelse skal den pågældende myndighed fremlægge dokumentation for, at der er begrundet mistanke om, at en person har begået en forbrydelse, at ransagningen, inspektionen eller beslaglæggelsen er nødvendig, og at de relevante genstande, der skal beslaglægges, findes (artikel 108, stk. 1, i strafferetsplejeloven). Selve kendelsen skal bl.a. indeholde navnet på den mistænkte for en forbrydelse og en beskrivelse af den strafbare handling, det sted, den person eller de genstande, der skal ransages, eller de genstande, der skal beslaglægges, udstedelsesdatoen og den faktiske anvendelsesperiode (artikel 114, stk. 1, sammenholdt med artikel 219 i CPA). Jf. bilag II, afsnit 2.2.1.2.

([206]) Når det er umuligt at indhente en kendelse på grund af situationens hastende karakter på gerningsstedet (artikel 216, stk. 3, i CPA), skal der efterfølgende straks indhentes en kendelse (artikel 216, stk. 3, i CPA).

([207]) Artikel 216, stk. 1 og 2, i CPA.

([208]) Artikel 218 i CPA. Som forklaret i afsnit 2.2.1.2 i bilag II antages frivilligt udleverede genstande desuden kun som bevismateriale i retssager, hvis der ikke er nogen rimelig tvivl om udleveringens frivillige karakter, hvilket det påhviler anklageren at bevise.

([209]) Artikel 321 i straffeloven.

([210]) Artikel 308-2 i CPA. Desuden kan en person (og dennes advokat) være til stede på tidspunktet for fuldbyrdelse af en kendelse om ransagning eller beslaglæggelse, og de kan derfor også gøre indsigelse på tidspunktet for fuldbyrdelse af kendelsen (artikel 121 og 219 i CPA).

([211]) Artikel 121 og 122 i CPA (om ransagninger) og artikel 219 sammenholdt med artikel 106, stk. 4, i CPA (om beslaglæggelser).

([212]) Se også bilag II, afsnit 2.2.2.1. Sådanne foranstaltninger kan træffes med tvungen bistand fra teleoperatører på grundlag af en skriftlig tilladelse fra en domstol (artikel 9, stk. 2, i CPPA), der udleveres til og opbevares af operatørerne (artikel 15-2 i CPPA og artikel 12 i CPPA-gennemførelsesdekretet). teleudbydere kan nægte at samarbejde, hvis oplysningerne om den overvågede person angivet i rettens skriftlige tilladelse (f.eks. den pågældendes telefonnummer) er ukorrekte, og de må under alle omstændigheder ikke videregive adgangskoder, der anvendes til telekommunikation (artikel 9, stk. 4, i CPPA).

([213]) Artikel 2, stk. 11, i CPPA.

([214]) Jf. artikel 2, stk. 6, i CPPA, hvor der henvises til »censur« (åbning af post uden den pågældende parts samtykke eller indsamling af viden om, optagelse eller tilbageholdelse af dens indhold ved brug af andre midler) og artikel 2, stk. 7, i CPPA, hvor der henvises til »aflytning« (indsamling eller optagelse af indholdet af telekommunikation ved at lytte til eller læse lyde, ord, symboler eller billeder i kommunikationen ved brug af elektroniske og mekaniske anordninger uden den pågældende parts samtykke eller gribe ind i deres transmission og modtagelse).

([215]) Artikel 13, stk. 1, i CPPA. Se også bilag II, afsnit 2.2.2.3. Desuden må realtidslokaliseringsdata og kommunikationsbekræftelsesdata vedrørende en bestemt basisstation kun indsamles med henblik på efterforskning af grov kriminalitet, eller hvis det ellers ville være vanskeligt at forhindre en forbrydelse eller indsamle bevismateriale (artikel 13, stk. 2, i CPPA). Dette afspejler behovet for at indføre yderligere garantier i tilfælde af foranstaltninger, der griber meget ind i privatlivets fred, i overensstemmelse med proportionalitetsprincippet.

([216]) Artikel 13 og 6 i CPPA.

([217]) Jf. artikel 13, stk. 3 og 9, i CPPA sammenholdt med artikel 6, stk. 4 og 6, i CPPA.

indhentes og meddeles teleudbyderen umiddelbart efter anmodningen om oplysningerne ([218]). Hvis retten efterfølgende nægter at give tilladelse, skal de indsamlede oplysninger tilintetgøres ([219]).

(157) Med hensyn til yderligere garantier for indsamling af kommunikationsbekræftelsesdata stiller CPPA særlige krav til registrering og gennemsigtighed ([220]). Både strafferetlige håndhævelsesmyndigheder ([221]) og teleudbydere ([222]) skal navnlig føre fortegnelser over fremsatte anmodninger og fremlagte oplysninger. Desuden skal strafferetlige håndhævelsesmyndigheder i princippet underrette de berørte personer om, at deres kommunikationsbekræftelsesdata er blevet indsamlet ([223]). En sådan underretning kan kun udsættes under ekstraordinære omstændigheder på grundlag af en tilladelse fra chefen for en kompetent distriktsadvokatur ([224]). En sådan tilladelse kan kun gives, hvis underretningen sandsynligvis vil 1) bringe den nationale sikkerhed og den offentlige sikkerhed og orden i fare, 2) forårsage død eller legemsbeskadigelse, 3) hindre en retfærdig rettergang (f.eks. føre til ødelæggelse af beviser eller trusler mod vidner) eller 4) ærekrænke den mistænkte, ofrene eller andre personer, der er indblandet i sagen, eller krænke deres privatliv. I så fald skal underretningen ske senest 30 dage efter, at årsagerne til udsættelsen ikke længere gør sig gældende ([225]). Efter underretningen har de berørte personer ret til at få oplysninger om begrundelsen for indsamlingen af deres oplysninger ([226]).

(158) Der gælder strengere regler for kommunikationsbegrænsende foranstaltninger, som kun må anvendes, hvis der er vægtige grunde til at formode, at visse former for grov kriminalitet, der er specifikt anført i CPPA, planlægges, begås eller er blevet begået ([227]). Kommunikationsbegrænsende foranstaltninger kan desuden kun træffes som en sidste udvej, og hvis det er vanskeligt at forhindre, at der begås en forbrydelse, at anholde en kriminel person eller at indsamle bevismateriale på anden vis ([228]). De skal straks bringes til ophør, når de ikke længere er nødvendige, for at sikre, at krænkelsen af privatlivets fred i forbindelse med kommunikation begrænses mest muligt ([229]). Oplysninger, der er indhentet ulovligt ved brug af kommunikationsbegrænsende foranstaltninger, antages ikke som bevismateriale i retssager eller disciplinærsager ([230]).

(159) Med hensyn til proceduremæssige garantier skal der i henhold til CPPA indhentes en retskendelse for at gennemføre kommunikationsbegrænsende foranstaltninger ([231]). I henhold til CPPA skal anmodningen om en kendelse og selve kendelsen indeholder detaljerede oplysninger ([232]), herunder om begrundelsen for anmodningen, og den kommunikation, der skal indsamles (hvilket skal være kommunikation til eller fra den mistænkte, som efterforskes) ([233]). Sådanne foranstaltninger kan kun træffes uden en kendelse i tilfælde af en overhængende fare for organiseret kriminalitet, eller hvis der er overhængende fare for anden grov kriminalitet, som kan forårsage

([218]) Artikel 13, stk. 2, i CPPA.
([219]) Artikel 13, stk. 3, i CPPA.
([220]) Jf. bilag II, afsnit 2.2.2.3.
([221]) Artikel 13, stk. 5 og 6, i CPPA.
([222]) Artikel 13, stk. 7, i CPPA. Desuden skal teleudbydere to gange om året aflægge rapport om videregivelsen af kommunikationsbekræftelsesdata til ministeriet for videnskab og IKT.
([223]) Jf. artikel 13-3, stk. 7, i CPPA sammenholdt med artikel 9-2 i CPPA. Personer skal navnlig underrettes senest 30 dage efter, at der er truffet afgørelse om (ikke) at rejse tiltale, eller senest et år og 30 dage efter, at der er truffet afgørelse om at suspendere en tiltale (selv om underretningen under alle omstændigheder skal ske senest et år og 30 dage efter indsamlingen af oplysningerne), jf. artikel 13-3, stk. 1, i CPPA.
([224]) Artikel 13-3, stk. 2-3, i CPPA.
([225]) Artikel 13-3, stk. 4, i CPPA.
([226]) Artikel 13-3, stk. 5, i CPPA. Efter anmodning fra den pågældende person skal anklageren eller kriminalpolitiet give en skriftlig begrundelse senest 30 dage efter modtagelsen af anmodningen, medmindre en af undtagelserne for udsættelse af underretning finder anvendelse (artikel 13-3, stk. 6, i CPPA).
([227]) F.eks. oprør, narkokriminalitet, sprængstofkriminalitet samt kriminalitet i forbindelse med den nationale sikkerhed, diplomatiske forbindelser eller militærbaser og -anlæg, jf. artikel 5, stk. 1, i CPPA. Se også bilag II, afsnit 2.2.2.2.
([228]) Artikel 3, stk. 2, og artikel 5, stk. 1, i CPPA.
([229]) Artikel 2 i CPPA-gennemførelsesdekretet.
([230]) Artikel 4 i CPPA.
([231]) Artikel 6, stk. 1, 2, 5-6, i CPPA.
([232]) En anmodning om en kendelse skal indeholde en beskrivelse af 1) de vægtige grunde til (prima facie) at formode, at en af de anførte former for kriminalitet planlægges, begås eller er blevet begået, samt eventuel dokumentation, 2) de kommunikationsbegrænsende foranstaltninger og deres mål, omfang, formål og varighed og 3) det sted, hvor foranstaltningerne vil blive gennemført, og hvordan de vil blive gennemført (artikel 6, stk. 4, i CPPA og artikel 4, stk. 1, i CPPA-gennemførelsesdekretet). I selve kendelsen angives foranstaltningerne samt deres mål, omfang, varighed, gennemførelsessted og gennemførelsesmetode (artikel 6, stk. 6, i CPPA).
([233]) Den kommunikationsbegrænsende foranstaltning skal være rettet mod specifikke brevforsendelser eller specifik telekommunikation, der sendes eller modtages af den mistænkte, eller brevforsendelser eller telekommunikation, der sendes eller modtages af den mistænkte i en bestemt periode (artikel 5, stk. 2, i CPPA).

direkte dødsfald eller alvorlig personskade, og der foreligger en nødsituation, som gør det umuligt at følge den almindelige procedure ([234]). I så fald skal en anmodning om en kendelse imidlertid indgives umiddelbart efter, at foranstaltningen er truffet ([235]). Kommunikationsbegrænsende foranstaltninger kan kun gennemføres i en periode på højst to måneder ([236]) og kan kun forlænges med rettens godkendelse, hvis betingelserne for at gennemføre foranstaltningerne fortsat er opfyldt ([237]). Den forlængede periode må ikke overstige et år eller tre år for visse former for særlig grov kriminalitet (f.eks. kriminalitet i forbindelse med oprør, aggression udefra og den nationale sikkerhed) ([238]).

(160) Som det er tilfældet ved indsamling af kommunikationsbekræftelsesdata, pålægger CPPA teleudbydere ([239]) og retshåndhævende myndigheder ([240]) at føre fortegnelser over gennemførelsen af kommunikationsbegrænsende foranstaltninger, og loven indeholder bestemmelser om underretning af den pågældende person, som under ekstraordinære omstændigheder kan udsættes, hvis det er nødvendigt af hensyn til vigtige samfundsinteresser ([241]).

(161) Endelig er manglende overholdelse af flere af begrænsningerne og garantierne i CPPA (herunder f.eks. forpligtelsen til at indhente en kendelse, registrering og underretning af den berørte person), både i forbindelse med indsamling af kommunikationsbekræftelsesdata og anvendelse af kommunikationsbegrænsende foranstaltninger, underlagt strafferetlige sanktioner ([242]).

(162) Strafferetlige håndhævelsesmyndigheders beføjelser til at indsamle kommunikationsdata på grundlag af CPPA (både kommunikationsindhold og kommunikationsbekræftelsesdata) er derfor afgrænset af klare og præcise regler og underlagt en række garantier. Disse garantier sikrer navnlig tilsyn med gennemførelsen af sådanne foranstaltninger, både forudgående (gennem forudgående retlig godkendelse) og efterfølgende (gennem registrerings- og rapporteringskrav), og letter berørte personers adgang til effektive retsmidler (ved at sikre, at de underrettes om indsamlingen af deres oplysninger).

3.2.1.3. Anmodninger om frivillig fremlæggelse af oplysninger af abonnentdata

(163) Ud over at basere sig på de obligatoriske foranstaltninger, der er beskrevet i betragtning 153-162, kan de koreanske retshåndhævende myndigheder anmode teleudbydere om at videregive »kommunikationsdata« på frivillig basis til støtte for en straffesag, efterforskning eller fuldbyrdelse af en dom (artikel 83, stk. 3, i TBA). Denne mulighed findes kun for begrænsede datasæt, dvs. brugernes navn, bopælsregistreringsnummer, adresse og telefonnummer, datoerne for brugernes tegning eller opsigelse af deres abonnement samt brugeridentifikationskoder (dvs. koder, der anvendes til at identificere den retmæssige bruger af computersystemer eller kommunikationsnet) ([243]). Da det kun personer, som indgår aftaler om tjenester direkte med en koreansk teleudbyder, der betragtes som »brugere« ([244]), vil EU-borgere, hvis oplysninger er blevet overført til Republikken Korea, normalt ikke falde ind under denne kategori ([245]).

(164) Der gælder forskellige begrænsninger for denne frivillige fremlæggelse af oplysninger, både for den retshåndhævende myndigheds udøvelse af beføjelser og for teleoperatørens svar. Som et generelt krav skal de retshåndhævende myndigheder handle i overensstemmelse med de forfatningsmæssige principper om nødvendighed og proportionalitet (forfatningens artikel 12, stk. 1, og artikel 37, stk. 2), herunder når de anmoder om frivillig videregivelse af oplysninger. Desuden skal de overholde PIPA, navnlig ved kun at indsamle personoplysninger i

([234]) Artikel 8, stk. 1, i CPPA. Indsamling af oplysninger i nødsituationer skal dog altid finde sted i overensstemmelse med en »erklæring om censur/aflytning i nødsituationer«, og den myndighed, der foretager indsamlingen, skal føre et register over alle hasteforanstaltninger (artikel 8, stk. 4, i CPPA).

([235]) Indsamlingen skal straks indstilles, hvis den retshåndhævende myndighed ikke indhenter en retskendelse inden for 36 timer (artikel 8, stk. 2, i CPPA), og i så fald vil de indsamlede oplysninger som forklaret i afsnit 2.2.2.2 i bilag II i princippet blive tilintetgjort. Retten skal også underrettes, hvis hasteforanstaltningerne er blevet afsluttet så hurtigt, at der ikke er behov for en tilladelse (f.eks. hvis den mistænkte anholdes umiddelbart efter påbegyndelsen af aflytningen, jf. artikel 8, stk. 5, i CPPA). I så fald skal retten have oplysninger om formål, mål, omfang, varighed, gennemførelsessted samt om begrundelsen for ikke at indgive en anmodning om en retskendelse (artikel 8, stk. 6-7, i CPPA).

([236]) Artikel 6, stk. 7, i CPPA. Hvis formålet med foranstaltningerne nås tidligere inden for denne frist, skal foranstaltningerne straks bringes til ophør.

([237]) Artikel 6, stk. 7-8, i CPPA.

([238]) Artikel 6, stk. 8, i CPPA.

([239]) Artikel 9, stk. 3, i CPPA.

([240]) Artikel 18, stk. 1, i CPPA-gennemførelsesdekretet.

([241]) Anklageren skal navnlig underrette den pågældende senest 30 dage efter tiltalerejsningen eller en afgørelse om ikke at rejse tiltale eller foretage anholdelse (artikel 9-2, stk. 1, i CPPA). Underretningen kan udsættes med godkendelse fra chefen for distriktsadvokaturen, hvis den sandsynligvis vil bringe den nationale sikkerhed i alvorlig fare eller forstyrre den offentlige orden, eller hvis den sandsynligvis vil påføre andres liv og legeme fysisk skade (artikel 9-2, stk. 4-6, i CPPA).

([242]) Artikel 16 og 17 i CPPA.

([243]) Artikel 83, stk. 3, i TBA. Se også bilag II, afsnit 2.2.3.

([244]) Artikel 2, stk. 9, i TBA.

([245]) Se også bilag II, afsnit 2.2.3.

det omfang, det er nødvendigt for at nå et legitimt formål, på en måde, der minimerer indvirkningen på den enkeltes ret til privatlivets fred (f.eks. artikel 3, stk. 1 og 6, i PIPA). Nærmere bestemt skal anmodningen om indhentning af kommunikationsdata på grundlag af TBA indgives skriftligt med angivelse af begrundelsen for anmodningen, linket til den relevante bruger og omfanget af de ønskede data ([246]).

(165) Teleudbydere er ikke forpligtet til at efterkomme sådanne anmodninger og må kun gøre det i overensstemmelse med PIPA. Dette betyder navnlig, at de skal afveje de forskellige berørte interesser, og de må ikke videregive oplysningerne, hvis dette sandsynligvis vil krænke den registreredes eller tredjemands interesser uretmæssigt ([247]). Dette vil f.eks. være tilfældet, hvis det er klart, at den anmodende myndighed har misbrugt sin myndighed ([248]). Teleoperatører skal føre fortegnelser over videregivelsen af oplysninger i henhold til TBA og aflægge rapport to gange om året til ministeren for videnskab og IKT ([249]).

(166) Desuden skal teleudbydere i henhold til afsnit 3 i meddelelse nr. 2021-5 (bilag I) i princippet underrette den berørte person, når de frivilligt efterkommer en anmodning ([250]). Dette vil gøre det muligt for den pågældende at udøve sine rettigheder og, hvis vedkommendes oplysninger videregives ulovligt, at indbringe en sag enten mod den dataansvarlige (f.eks. for at videregive oplysningerne i strid med PIPA eller for at efterkomme en anmodning, der var klart uforholdsmæssig) eller mod den retshåndhævende myndighed (f.eks. for at gå ud over, hvad der er nødvendigt og forholdsmæssigt, eller for ikke at overholde de proceduremæssige krav i TBA).

3.2.2. *Yderligere anvendelse af de indsamlede oplysninger*

(167) Behandlingen af personoplysninger, der indsamles af koreanske strafferetlige håndhævelsesmyndigheder, skal opfylde alle kravene i PIPA, herunder med hensyn til formålsbegrænsning (artikel 3, stk. 1-2, i PIPA), lovlig anvendelse og videregivelse til tredjemand (artikel 15, 17 og 18 i PIPA), internationale overførsler (artikel 17 og 18 i PIPA sammenholdt med afsnit 2 i meddelelse nr. 2021-5) ([251]), proportionalitet og dataminimering (artikel 3, stk. 1 og 6, i PIPA) og opbevaringsbegrænsning (artikel 21 i PIPA) ([252]).

(168) Hvad angår indholdet af kommunikation, der erhverves via gennemførelse af kommunikationsbegrænsende foranstaltninger, begrænser CPPA specifikt den mulige anvendelse heraf til efterforskning, retsforfølgelse eller forebyggelse af grov kriminalitet ([253]), disciplinærsager i forbindelse med denne kriminalitet, erstatningskrav rejst af en part i kommunikationen, eller hvor dette er specifikt tilladt i henhold til anden lovgivning ([254]). Desuden må det indsamlede indhold af telekommunikation, der overføres via internettet, kun opbevares med godkendelse fra den domstol, der godkendte de kommunikationsbegrænsende foranstaltninger ([255]), med henblik på at anvende det til efterforskning, retsforfølgelse eller forebyggelse af grov kriminalitet ([256]). Mere generelt forbyder CPPA videregivelse af fortrolige oplysninger, der er indhentet ved kommunikationsbegrænsende foranstaltninger, og anvendelse af sådanne oplysninger til skade for de af foranstaltningerne omfattede personers omdømme ([257]).

3.2.3. *Tilsyn*

(169) I Korea overvåges strafferetlige håndhævelsesmyndigheders aktiviteter af forskellige organer ([258]).

([246]) Artikel 83, stk. 4, i TBA. Hvis det på grund af sagens hastende karakter er umuligt at indgive en skriftlig anmodning, skal den skriftlige anmodning indgives, så snart der ikke længere er nogen begrundelse for sagens hastende karakter (artikel 83, stk. 4, i TBA).

([247]) Artikel 18, stk. 2, i PIPA.

([248]) Højesterets afgørelse 2012Da105482 af 10. marts 2016. Se også bilag II, afsnit 2.2.3, om denne højesteretsafgørelse.

([249]) Artikel 83, stk. 5-6, i TBA.

([250]) Dette krav er underlagt begrænsede og kvalificerede undtagelser, navnlig hvis og så længe underretningen vil bringe en igangværende strafferetlig efterforskning i fare eller sandsynligvis vil skade en anden persons liv eller legeme, hvis disse rettigheder eller interesser går klart forud for den registreredes rettigheder. Jf. afsnit 3, nr. iii) 1), i meddelelsen.

([251]) De koreanske offentlige myndigheder skal navnlig gennem et retligt bindende instrument sikre et beskyttelsesniveau, som svarer til niveauet i PIPA, se også betragtning 90.

([252]) Se også bilag II, afsnit 1.2.

([253]) Jf. betragtning 158.

([254]) Artikel 12 i CPPA. Jf. bilag II, afsnit 2.2.2.2.

([255]) Anklageren eller politiet, der gennemfører de kommunikationsbegrænsende foranstaltninger, skal udvælge den telekommunikation, der skal opbevares, senest 14 dage efter foranstaltningernes udløb, og anmode om rettens godkendelse (i tilfælde af politiets indgriben skal anmodningen indgives til en anklager, som derefter indgiver den til retten), jf. artikel 12-2, stk. 1 og 2, i CPPA.

([256]) En anmodning om en sådan godkendelse skal indeholde oplysninger om de kommunikationsbegrænsende foranstaltninger, et resumé af resultaterne af foranstaltningerne, begrundelsen for opbevaringen (sammen med dokumentation) og oplysninger om den telekommunikation, der skal opbevares (artikel 12-2, stk. 3, i CPPA). Hvis der ikke indgives en anmodning, skal de indsamlede oplysninger slettes senest 14 dage efter udløbet af den kommunikationsbegrænsende foranstaltning (artikel 12-2, stk. 5, i CPPA), og hvis anmodningen afslås, senest syv dage herefter (artikel 12-2, stk. 5, i CPPA). I begge tilfælde skal der indgives en rapport om sletningen til den domstol, der godkendte indsamlingen, senest syv dage herefter.

([257]) Artikel 11, stk. 2, i CPPA-gennemførelsesdekretet.

([258]) Jf. bilag II, afsnit 2.3.

(170) For det første er politiet underlagt internt tilsyn foretaget af en generalinspektør ([259]), som fører legalitetskontrol, herunder med hensyn til mulige krænkelser af menneskerettighederne. Generalinspektøren blev oprettet for at gennemføre lov om revisioner i den offentlige sektor, som tilskynder til oprettelse af selvrevisionsorganer og fastsætter specifikke krav til deres sammensætning og opgaver. Det fastsættes navnlig i loven, at lederen af et selvrevisionsorgan skal hentes uden for den relevante myndighed (f.eks. tidligere dommere, professorer) og udnævnes for en periode på to til fem år ([260]), at lederen kun kan afskediges af velbegrundede årsager (f.eks. hvis vedkommende ikke kan varetage sine opgaver af helbredsmæssige årsager eller er genstand for disciplinære foranstaltninger) ([261]), og at lederen er garanteret uafhængighed i videst muligt omfang ([262]). Hindring af selvrevision straffes med administrative bøder ([263]). Revisionsrapporter (som kan omfatte henstillinger, anmodninger om disciplinære foranstaltninger og anmodninger om erstatning eller berigtigelse) fremsendes til lederen af den relevante offentlige myndighed, revisions- og inspektionsudvalget (BAI) ([264]) og offentliggøres generelt ([265]). Resultaterne af rapportens gennemførelse skal også meddeles BAI ([266]) (jf. betragtning 173 om BAI's tilsynsrolle og beføjelser).

(171) For det andet fører PIPC tilsyn med, at strafferetlige håndhævelsesmyndigheders databehandling er i overensstemmelse med PIPA og andre love, der beskytter den enkeltes ret til privatlivets fred, herunder de love, der regulerer indsamling af (elektronisk) bevismateriale med henblik på strafferetlig håndhævelse, som beskrevet i afsnit 3.2.1 ([267]). Da PIPC's tilsyn omfatter en undersøgelse af lovligheden og rimeligheden af dataindsamlingen og -behandlingen (artikel 3, stk. 1, i PIPA), som vil blive overtrådt, hvis personoplysninger tilgås og anvendes i strid med disse love ([268]), kan PIPC navnlig også undersøge og håndhæve overholdelsen af de begrænsninger og garantier, der er beskrevet i afsnit 3.2.1 ([269]). Ved udøvelsen af denne tilsynsrolle kan PIPC gøre brug af alle sine undersøgelsesbeføjelser og afhjælpende beføjelser som nærmere beskrevet i afsnit 2.4.2. Allerede inden den nylige reform af PIPA (dvs. i forbindelse med PIPC's tidligere tilsyn med den offentlige sektor) udførte PIPC en række tilsyn med strafferetlige håndhævelsesmyndigheders behandling af personoplysninger, f.eks. i forbindelse med afhøring af mistænkte (sag nr. 2013-16 af 26. august 2013), med hensyn til fremsendelse af meddelelser til enkeltpersoner om pålæggelse af administrative bøder (sag nr. 2015-02-04 af 26. januar 2015), udveksling af oplysninger med andre myndigheder (sag nr. 2018-15-146 af 9. juli 2018, sag nr. 2018-25-308 af 10. december 2018, sag nr. 2019-02-015, 29. januar 2019), indsamling af fingeraftryk eller fotografier (sag nr. 2019-17-273 af 9. september 2019), anvendelse af droner (sag nr. 2020-01-004 af 13. januar 2020). I disse sager undersøgte PIPC overholdelsen af flere bestemmelser i PIPA (f.eks. lovligheden af behandlingen, principperne om formålsbegrænsning og dataminimering), men også relevante bestemmelser i andre love såsom strafferetsplejeloven, og udstedte om nødvendigt henstillinger om at bringe behandlingen i overensstemmelse med databeskyttelseskravene.

(172) For det tredje føres der uafhængigt tilsyn af den nationale menneskerettighedskommission (NHRC) ([270]), som kan undersøge krænkelser af retten til privatlivets fred og privatlivets fred i forbindelse med korrespondance som led i dens generelle mandat til at beskytte de grundlæggende rettigheder i forfatningens artikel 10-22. NHRC består af 11 kommissærer, der skal opfylde specifikke kvalifikationskriterier ([271]) og udpeges af præsidenten i overensstemmelse med de procedurer, der er fastsat ved lov. Fire kommissærer udnævnes efter indstilling fra nationalforsamlingen, fire efter indstilling fra præsidenten og tre efter indstilling fra højesteretspræsidenten ([272]). Formanden udnævnes af præsidenten blandt kommissærerne, og udnævnelsen skal bekræftes af nationalforsamlingen ([273]). Kommissærer (herunder formanden) udnævnes for en periode på tre år, der kan forlænges, og kan kun afsættes, hvis de idømmes fængselsstraf eller ikke længere er i stand til at varetage deres opgaver på grund

([259]) Jf. bilag II, afsnit 2.3.1. Se også https://www.police.go.kr/eng/knpa/org/org01.jsp.
([260]) På samme måde udnævnes revisorer på grundlag af specifikke betingelser i loven, jf. artikel 16 ff. i lov om revisioner i den offentlige sektor.
([261]) Artikel 8-11 i lov om revisioner i den offentlige sektor.
([262]) Artikel 7 i lov om revisioner i den offentlige sektor.
([263]) Artikel 41 i lov om revisioner i den offentlige sektor.
([264]) Artikel 23, stk. 1, i lov om revisioner i den offentlige sektor.
([265]) Artikel 26 i lov om revisioner i den offentlige sektor.
([266]) Artikel 23, stk. 3, i lov om revisioner i den offentlige sektor.
([267]) Jf. artikel 7-8, stk. 3 og 4, og artikel 7-9, stk. 5, i PIPA.
([268]) Jf. PIPC-meddelelse nr. 2021-5, afsnit 6 (bilag I).
([269]) Se også bilag II, afsnit 2.3.4.
([270]) Artikel 1 i lov om menneskerettighedskommissionen (NHRC-loven).
([271]) For at blive udnævnt skal en kommissær 1) have været ansat ved et universitet eller et godkendt forskningsinstitut i mindst ti år, som minimum på lektorniveau, 2) have udøvet hvervet som dommer, anklager eller advokat i mindst ti år, 3) have været involveret i menneskerettighedsaktiviteter i mindst ti år (f.eks. for en nonprofitorganisation, ikkestatslig organisation eller international organisation) eller 4) være blevet anbefalet af civilsamfundsgrupper (artikel 5, stk. 3, i NHRC-loven). Desuden må kommissærerne efter udnævnelsen ikke bestride et sideløbende hverv i nationalforsamlingen, lokalråd eller en statslig eller lokal myndighed (som offentligt ansat), jf. artikel 10 i NHRC-loven.
([272]) Artikel 5, stk. 1 og 2, i NHRC-loven.
([273]) Jr. artikel 5, stk. 5, i NHRC-loven.

af langvarig psykisk eller fysisk sygdom (i så fald skal to tredjedele af kommissærerne være enige i afsættelsen) ([274]). Som led i en undersøgelse kan NHRC anmode om fremlæggelse af relevant materiale, foretage inspektioner og indkalde enkeltpersoner til at afgive vidneforklaring ([275]). Med hensyn til afhjælpende beføjelser kan NHRC udstede (offentlige) henstillinger for at forbedre eller korrigere specifikke politikker og praksis, som offentlige myndigheder skal følge op på med et forslag til gennemførelsesplan ([276]). Hvis den pågældende myndighed undlader at gennemføre henstillingerne, skal den underrette kommissionen herom ([277]), som derefter kan underrette nationalforsamlingen om denne undladelse og/eller offentliggøre den. Ifølge den koreanske regerings officielle redegørelse (afsnit 2.3.5 i bilag II) efterlever de koreanske myndigheder generelt NHRC's henstillinger og har et stærkt incitament hertil, da deres gennemførelse er blevet vurderet som led i en generel, løbende evaluering, som premierministerens kontor fører tilsyn med. Årlige tal for NHRC's aktiviteter viser, at NHRC fører aktivt tilsyn med strafferetlige håndhævelsesmyndigheders aktiviteter, enten på grundlag af individuelle klager eller undersøgelser på eget initiativ ([278]).

(173) For det fjerde udføres det generelle tilsyn med lovligheden af de offentlige myndigheders aktiviteter af BAI, som undersøger statens indtægter og udgifter, men også mere generelt fører tilsyn med, at offentlige myndigheder overholder deres forpligtelser, for at forbedre den offentlige forvaltnings funktion ([279]). BAI er formelt oprettet under Republikken Koreas præsident, men varetager sine opgaver uafhængigt ([280]). Udvalgets beføjelser til at ansætte, afskedige og organisere sit personale og udarbejde budget udøves desuden i fuld uafhængighed ([281]). BAI består af en formand (udnævnt af præsidenten med nationalforsamlingens samtykke ([282])) og seks kommissærer (udpeget af præsidenten efter indstilling fra formanden ([283])), som skal opfylde specifikke lovbestemte kvalifikationskriterier ([284]) og kun kan afsættes i tilfælde af forfald, fængselsstraf eller manglende evne til at varetage deres opgaver på grund af langvarig psykisk eller fysisk sygdom ([285]). BAI foretager en generel revision en gang om året, men kan også foretage specifikke revisioner af spørgsmål af særlig interesse. I forbindelse med en revision eller inspektion kan BAI anmode om fremlæggelse af dokumenter og indkalde enkeltpersoner ([286]). BAI kan udstede henstillinger, anmode om disciplinære foranstaltninger eller indgive en anmeldelse ([287]).

(174) Endelig fører nationalforsamlingen parlamentarisk kontrol med offentlige myndigheder gennem undersøgelser og inspektioner ([288]) af deres aktiviteter ([289]). Den kan anmode om fremlæggelse af dokumenter, pålægge vidner at give møde ([290]), henstille, at der træffes korrigerende foranstaltninger (hvis den konkluderer, at der har fundet

([274]) Artikel 7, stk. 1, og artikel 8 i NHRC-loven.
([275]) Artikel 36 i NHRC-loven. I henhold til lovens artikel 6, stk. 7, kan fremlæggelse af materiale eller genstande afvises, hvis det vil krænke den fortrolige karakter af statslige forhold, der kan have væsentlig indvirkning på statens sikkerhed eller diplomatiske forbindelser eller vil udgøre en alvorlig hindring for en strafferetlig efterforskning eller verserende retssag. I sådanne tilfælde kan Kommissionen anmode lederen af det relevante organ (som skal overholde reglerne i god tro) om yderligere oplysninger, hvis det er nødvendigt for at gøre det muligt at undersøge, om afslaget på at fremlægge oplysningerne er berettiget.
([276]) Jf. artikel 25, stk. 1 og 3, i NHRC-loven.
([277]) Jf. artikel 25, stk. 4, i NHRC-loven.
([278]) F.eks. modtog NHRC i perioden 2015-2019 årligt mellem 1 380 og 1 699 klager over strafferetlige håndhævelsesmyndigheder og behandlede et tilsvarende højt antal (NHRC behandlede f.eks. 1 546 klager mod politiet i 2018 og 1 249 i 2019). NHRC gennemførte også flere undersøgelser på eget initiativ som nærmere beskrevet i NHRC's årsrapport for 2018 (findes på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7602641) og årsrapporten for 2019 (findes på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([279]) Artikel 20 og 24 i lov om revisions- og inspektionsudvalget (BAI-loven). Jf. bilag II, afsnit 2.3.2.
([280]) Artikel 2, stk. 1, i BAI-loven.
([281]) Artikel 2, stk. 2, i BAI-loven.
([282]) Artikel 4, stk. 1, i BAI-loven.
([283]) Artikel 5, stk. 1, og artikel 6 i BAI-loven.
([284]) Har f.eks. udøvet hvervet som dommer, offentlig anklager eller advokat i mindst ti år, arbejdet som embedsmand, professor eller i en højere stilling ved et universitet i mindst otte år eller arbejdet i mindst ti år i et børsnoteret selskab eller en statsejet institution (heraf mindst fem år som leder), jf. artikel 7 i BAI-loven. Kommissærer må desuden ikke deltage i politiske aktiviteter og sideløbende bestride hverv i nationalforsamlingen, forvaltningsorganer, organisationer, der er underlagt BAI's revision og inspektion, eller andre lønnede hverv eller stillinger (artikel 9 i BAI-loven).
([285]) Artikel 8 i BAI-loven.
([286]) Jf. f.eks. artikel 27 i BAI-loven.
([287]) Artikel 24 og 31-35 i BAI-loven.
([288]) Artikel 128 i lov om nationalforsamlingen og artikel 2, 3 og 15 i lov om inspektion og undersøgelse af statsforvaltningen. Dette omfatter årlige inspektioner af regeringsanliggender som helhed, men også undersøgelser af specifikke spørgsmål.
([289]) Jf. bilag, afsnit 2.2.3.
([290]) Artikel 10, stk. 1, i lov om inspektion og undersøgelse af statsforvaltningen. Se også artikel 128 og 129 i lov om nationalforsamlingen.

ulovlige eller uretmæssige aktiviteter sted) ([291]) og offentliggøre resultaterne af sine undersøgelser ([292]). Hvis nationalforsamlingen anmoder om, at der træffes korrigerende foranstaltninger — hvilket f.eks. kan omfatte tildeling af erstatning, iværksættelse af disciplinære foranstaltninger eller forbedring af interne procedurer — er den pågældende offentlige myndighed forpligtet til at handle straks og aflægge rapport om resultatet til nationalforsamlingen ([293]).

3.2.4. *Klageadgang*

(175) I det koreanske system er der forskellige (retlige) prøvelsesmekanismer, herunder mulighed for at opnå skadeserstatning.

(176) For det første giver PIPA enkeltpersoner ret til indsigt i og berigtigelse, sletning og suspension af behandlingen af personoplysninger, der behandles med henblik på strafferetlig håndhævelse ([294]).

(177) For det andet kan enkeltpersoner gøre brug af de forskellige prøvelsesmekanismer i henhold til PIPA, hvis deres oplysninger er blevet behandlet af en strafferetlig håndhævelsesmyndighed i strid med PIPA eller i strid med de begrænsninger og garantier, der gælder for indsamling af personoplysninger i andre love (dvs. CPA eller CPPA, jf. betragtning 171). Enkeltpersoner kan navnlig indgive en klage til PIPC (herunder via callcentret for privatlivsbeskyttelse, der drives af Koreas internet- og sikkerhedsagentur ([295])) eller til udvalget for bilæggelse af tvister om personoplysninger ([296]). Disse klagemuligheder er ikke underlagt yderligere krav om antagelighed. På grundlag af lov om forvaltningssager kan enkeltpersoner desuden påklage/anfægte PIPC's afgørelser eller manglende handling (jf. betragtning 132).

(178) For det tredje kan enhver ([297]) indgive en klage til NHRC vedrørende en koreansk strafferetlig håndhævelsesmyndigheds krænkelse af retten til privatlivets fred og databeskyttelse. NHRC kan fremsætte henstillinger om ændring eller forbedring af enhver relevant lov, institution, politik eller praksis ([298]) eller gennemførelse af foranstaltninger såsom mægling ([299]), ophør af krænkelsen af menneskerettighederne, skadeserstatning og foranstaltninger til at forhindre, at de samme eller lignende krænkelser gentager sig ([300]). Ifølge den koreanske regerings officielle redegørelse (afsnit 2.4.2 i bilag II) kan dette også omfatte sletning af ulovligt indsamlede personoplysninger. NHRC har ikke beføjelse til at træffe bindende afgørelser, men der er tale om en mere uformel, billig og let tilgængelig klageadgang, navnlig fordi der som forklaret i bilag II, afsnit 2.4.2, ikke stilles krav om påvisning af en faktisk skade, inden klagen kan undersøges ([301]). Dette sikrer, at klager fra enkeltpersoner vedrørende indsamlingen af deres oplysninger kan undersøges, selv om de pågældende ikke kan påvise, at deres oplysninger rent faktisk er blevet indsamlet (f.eks. fordi de endnu ikke er blevet underrettet). Det fremgår af NHRC's årlige aktivitetsrapporter, at enkeltpersoner også gør brug af denne mulighed i praksis for at anfægte strafferetlige håndhævelsesmyndigheders aktiviteter, herunder deres behandling af personoplysninger ([302]). Hvis en person ikke er tilfreds med udfaldet af proceduren for NHRC, kan vedkommende anfægte NHRC's afgørelser

([291]) Artikel 16, stk. 2, i lov om inspektion og undersøgelse af statsforvaltningen.
([292]) Artikel 12-2 i lov om inspektion og undersøgelse af statsforvaltningen.
([293]) Artikel 16, stk. 3, i lov om inspektion og undersøgelse af statsforvaltningen.
([294]) Denne ret kan udøves direkte over for den kompetente myndighed eller indirekte via PIPC (artikel 35, stk. 2, i PIPA). Som nærmere beskrevet i betragtning 76-78 finder undtagelser fra disse rettigheder kun anvendelse, når det er nødvendigt for at beskytte vigtige (offentlige) interesser.
([295]) Artikel 62 i PIPA.
([296]) Artikel 40-50 i PIPA og artikel 48-2 til 57 i PIPA-gennemførelsesdekretet. Se også bilag II, afsnit 2.4.1.
([297]) Som forklaret i bilag II, afsnit 2.4.2, skal udtrykket »bosiddende« ses i sammenhæng med begrebet »jurisdiktion« og ikke »område«, selv om der i artikel 4 i NHRC-loven henvises til statsborgere og udlændinge, der er bosiddende i Republikken Korea. Hvis en udlændings grundlæggende rettigheder krænkes af nationale institutioner i Korea, kan den pågældende derfor indgive en klage til NHRC. Dette ville være tilfældet, hvis de koreanske offentlige myndigheder ulovligt tilgår personoplysninger om en udlænding, der er overført til Korea. Jf. navnlig forklaringerne på https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2.
([298]) Artikel 44 i NHRC-loven.
([299]) En person kan også anmode om at få afgjort klagesagen gennem mægling, jf. artikel 42 ff. i NHRC-loven.
([300]) Jf. artikel 42, stk. 4, i NHRC-loven. NHRC kan desuden vedtage hasteforanstaltninger i forbindelse med en igangværende overtrædelse, der sandsynligvis vil forårsage skade, som er vanskelig at afhjælpe, hvis der ikke gribes ind, jf. artikel 48 i NHRC-loven.
([301]) En klage skal i princippet indgives inden for et år efter krænkelsen, men NHRC kan stadig beslutte at undersøge en klage, der indgives efter denne frist, så længe forældelsesfristen i henhold til straffe- eller civilretten ikke er udløbet (artikel 32, stk. 1, nr. 4, i NHRC-loven).
([302]) NHRC har f.eks. tidligere behandlet klager og fremsat henstillinger om ulovlige beslaglæggelser og en overtrædelse af kravet om at underrette de berørte personer om en beslaglæggelse (se s. 80 og 91 i NHRC's årsrapport for 2018, som findes på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746), og om politiets, anklagemyndighedens og domstolenes ulovlige behandling af personoplysninger (se s. 157-158 i NHRC's årsrapport for 2019, som findes på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7603308, og s. 76 i årsrapporten for 2019, som findes på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).

(f.eks. en afgørelse om ikke at fortsætte undersøgelsen af en klage ([303])) og henstillinger ved de koreanske domstole i henhold til lov om forvaltningssager (jf. betragtning 181) ([304]). En procedure for NHRC kan desuden lette adgangen til domstolene yderligere, da en person kan anlægge sag mod den offentlige myndighed, der har behandlet vedkommendes oplysninger ulovligt, på grundlag af NHRC's konklusioner og i overensstemmelse med de procedurer, der er beskrevet i betragtning 181-183.

(179) Endelig findes der forskellige retsmidler, som giver enkeltpersoner mulighed for at påberåbe sig de begrænsninger og garantier, der er beskrevet i afsnit 3.2.1, ved at få prøvet deres sag ved domstolene ([305]).

(180) Med hensyn til beslaglæggelse (herunder af oplysninger) giver CPA mulighed for at gøre indsigelse mod eller anfægte fuldbyrdelsen af en kendelse gennem en »kvasiklagemekanisme« ved at indgive en anmodning til den kompetente ret om at annullere eller ændre en disposition truffet af en anklager eller politiet ([306]).

(181) Mere generelt kan enkeltpersoner anfægte offentlige myndigheders (herunder strafferetlige håndhævelsesmyndigheders) handlinger ([307]) eller undladelser ([308]) i henhold til lov om forvaltningssager ([309]). En administrativ foranstaltning betragtes som en »anfægtelig disposition«, hvis den har direkte indvirkning på borgerlige rettigheder og pligter ([310]), hvilket, som bekræftet af den koreanske regering (afsnit 2.4.3 i bilag II), er tilfældet for foranstaltninger til indsamling af personoplysninger, enten direkte (f.eks. ved aflytning af kommunikation), gennem bindende anmodninger om videregivelse (f.eks. til en tjenesteudbyder) eller anmodninger om frivilligt samarbejde. Hvis en klage i henhold til lov om forvaltningssager skal antages til realitetsbehandling, skal den pågældende person have en retlig interesse i at forfølge kravet ([311]). Ifølge højesterets retspraksis fortolkes »retlig interesse« som en »retligt beskyttet interesse«, dvs. en direkte og specifik interesse, der er beskyttet af love og forskrifter, som administrative bestemmelser er baseret på (dvs. ikke offentlighedens generelle, indirekte og abstrakte interesser) ([312]). Enkeltpersoner har en sådan retlig interesse i tilfælde af overtrædelse af de begrænsninger og garantier, der gælder for indsamling af deres personoplysninger med henblik på strafferetlig håndhævelse (i henhold til specifik lovgivning eller PIPA). På grundlag af lov om forvaltningssager kan en domstol beslutte at tilbagekalde eller ændre en ulovlig disposition, udstede en afgørelse om ugyldighed (dvs. en afgørelse om, at dispositionen ikke har retsvirkning eller ikke eksisterer i retsordenen) eller udstede en afgørelse om, at en undladelse er ulovlig ([313]). En endelig dom i henhold til lov om forvaltningssager er bindende for parterne ([314]).

([303]) Hvis NHRC f.eks. undtagelsesvis ikke har mulighed for at inspicere visse materialer eller faciliteter, fordi de vedrører statshemmeligheder, der kan have en væsentlig indvirkning på statens sikkerhed eller diplomatiske forbindelser, eller hvis inspektionen vil udgøre en alvorlig hindring for en strafferetlig efterforskning eller verserende retssag, og hvis dette forhindrer NHRC i at foretage den nødvendige undersøgelse for at vurdere, om den modtagne klage er begrundet, underretter udvalget den pågældende om begrundelsen for, at klagen blev afvist, i overensstemmelse med artikel 39 i NHRC-loven. I dette tilfælde kan den pågældende anfægte NHRC's afgørelse i henhold til lov om forvaltningssager.

([304]) Jf. f.eks. Seoul High Courts afgørelse 2007NU27259 af 18. april 2008, stadfæstet ved højesterets afgørelse 2008Du7854 af 9. oktober 2008, og Seoul High Courts afgørelse nr. 2017Nu69382 af 2. februar 2018.

([305]) Jf. bilag II, afsnit 2.4.3.

([306]) Artikel 417 i CPA sammenholdt med artikel 414, stk. 2, i CPA. Se også højesterets afgørelse nr. 97Mo66 af 29. september 1997.

([307]) I lov om forvaltningssager henvises til en »disposition«, dvs. udøvelse af eller afvisning af at udøve offentlig myndighed i en konkret sag.

([308]) I lov om forvaltningssager forstås herved et forvaltningsorgans langvarige undladelse af at træffe en bestemt disposition i strid med en retlig forpligtelse hertil.

([309]) En administrativ klage kan i første omgang indbringes for administrative klageudvalg, der er nedsat under visse offentlige myndigheder (f.eks. NIS og NHRC), eller for det centrale administrative klageudvalg, der er nedsat under kommissionen for korruptionsbekæmpelse og borgerlige rettigheder (artikel 6 i lov om administrative klager og artikel 18, stk. 1, i lov om forvaltningssager), som en mere uformel klagemulighed. Et krav kan dog også indbringes direkte for de koreanske domstole på grundlag af lov om forvaltningssager.

([310]) Højesterets afgørelse 98Du18435 af 22. oktober 1999, højesterets afgørelse 99Du1113 af 8. september 2000 og højesterets afgørelse 2010Du3541 af 27. september 2012.

([311]) Artikel 12, 35 og 36 i lov om forvaltningssager. Desuden skal en anmodning om tilbagekaldelse/ændring af en disposition og en anmodning om at få fastslået, at en undladelse er ulovlig, indgives senest 90 dage efter den dato, hvor personen får kendskab til dispositionen/undladelsen, og i princippet senest et år efter datoen for udstedelsen af dispositionen eller datoen for undladelsen, medmindre der er berettigede grunde (artikel 20 og artikel 38, stk. 2, i lov om forvaltningssager). Begrebet »berettigede grunde« er blevet fortolket bredt af højesteret og kræver en vurdering af, om det er samfundsmæssigt acceptabelt at give mulighed for at indbringe en forsinket klage i lyset af alle sagens omstændigheder (højesterets afgørelse 90NU6521 af 28. juni 1991). Som bekræftet af den koreanske regering i afsnit 2.4.3 i bilag II omfatter dette (men er ikke begrænset til) årsager til forsinkelser, som den pågældende part ikke kan holdes ansvarlig for (dvs. situationer, der ligger uden for klagerens kontrol, f.eks. hvis vedkommende ikke er blevet underrettet om indsamlingen af sine personoplysninger) eller force majeure (f.eks. en naturkatastrofe eller krig).

([312]) Højesterets afgørelse 2006Du330 af 26. marts 2006.

([313]) Artikel 2 og 4 i lov om forvaltningssager.

([314]) Artikel 30, stk. 1, i lov om forvaltningssager.

(182) Ud over at anfægte statslige foranstaltninger ved at anlægge en forvaltningssag kan enkeltpersoner også indgive en forfatningsmæssig klage til forfatningsdomstolen vedrørende enhver krænkelse af deres grundlæggende rettigheder som følge af udøvelse eller manglende udøvelse af offentlig myndighed (undtagen domstolsafgørelser) ([315]). Hvis der findes andre retsmidler, skal disse først udtømmes. I henhold til forfatningsdomstolens retspraksis kan udenlandske statsborgere indgive en forfatningsmæssig klage, i det omfang deres grundlæggende rettigheder er anerkendt i den koreanske forfatning (se forklaringerne i afsnit 1.1) ([316]). Forfatningsdomstolen kan ugyldiggøre den udøvelse af offentlig myndighed, der forårsagede overtrædelsen, eller fastslå, at en bestemt undladelse af at handle er forfatningsstridig ([317]). I så fald er den relevante myndighed forpligtet til at træffe foranstaltninger for at efterkomme domstolens afgørelse.

(183) Personer kan desuden opnå skadeserstatning ved de koreanske domstole. Dette omfatter først og fremmest muligheden for at kræve erstatning for overtrædelser af PIPA begået af strafferetlige håndhævelsesmyndigheder i overensstemmelse med artikel 39 (se også betragtning 135). Mere generelt kan enkeltpersoner søge erstatning for skade, som offentligt ansatte har forvoldt under udøvelsen af deres officielle hverv i strid med loven, på grundlag af lov om erstatning fra staten (se også betragtning 135) ([318]).

(184) De mekanismer, der er beskrevet i betragtning 176-183, giver de registrerede adgang til effektive administrative og retlige klagemuligheder, der navnlig sætter dem i stand til at håndhæve deres rettigheder, herunder retten til at få adgang til deres personoplysninger eller til at få sådanne oplysninger berigtiget eller slettet.

3.3. **De koreanske offentlige myndigheders adgang til og anvendelse af personoplysninger til nationale sikkerhedsformål**

(185) Republikken Koreas lovgivning indeholder en række begrænsninger og garantier for adgangen til og anvendelsen af personoplysninger til nationale sikkerhedsformål og indeholder en række tilsyns- og prøvelsesmekanismer, som er i overensstemmelse med de krav, der er omhandlet i betragtning 141-143 i denne afgørelse. De betingelser, hvorunder en sådan adgang kan finde sted, og de garantier, der gælder for udøvelsen af disse beføjelser, vurderes nærmere i de følgende afsnit.

3.3.1. *Retsgrundlag, begrænsninger og garantier*

(186) I Republikken Korea kan der gives adgang til personoplysninger til nationale sikkerhedsformål på grundlag af CPPA, TBA og lov om bekæmpelse af terrorisme og beskyttelse af borgerne og den offentlige sikkerhed (anti-terrorloven) ([319]). Den vigtigste myndighed ([320]) med kompetence inden for national sikkerhed er den nationale efterretningstjeneste (NIS) ([321]). NIS skal i forbindelse med indsamling og anvendelse af personoplysninger

([315]) Artikel 68, stk. 1, i lov om forfatningsdomstolen. Forfatningsmæssige klager skal indgives senest 90 dage efter, at den pågældende har fået kendskab til overtrædelsen, og senest et år efter, at den er begået. Som det også forklares i bilag II, afsnit 2.4.3, vil en klage stadig kunne antages til realitetsbehandling, hvis der foreligger »berettigede grunde« som fortolket i overensstemmelse med højesterets retspraksis beskrevet i fodnote 312, da proceduren i lov om forvaltningssager finder anvendelse på tvister i henhold til artikel 40 i lov om forfatningsdomstolen. Hvis andre retsmidler først skal udtømmes, skal der indgives en forfatningsmæssig klage senest 30 dage efter den endelige afgørelse om et sådant retsmiddel (artikel 69 i lov om forfatningsdomstolen).

([316]) Forfatningsdomstolens afgørelse nr. 99HeonMa194 af 29. november 2001.

([317]) Artikel 75, stk. 3, i lov om forfatningsdomstolen.

([318]) Artikel 2, stk. 1, i lov om erstatning fra staten.

([319]) Jf. bilag II, afsnit 3.1.

([320]) Politiet og anklagemyndigheden kan også undtagelsesvis indsamle personoplysninger til nationale sikkerhedsformål (jf. fodnote 327 og bilag II, afsnit 3.2.1.2). Desuden har Koreas militære efterretningsagentur (forsvarssikkerhedskommandoen oprettet under forsvarsministeriet) beføjelser på det nationale sikkerhedsområde. Som forklaret i bilag II, afsnit 3.1, har agenturet imidlertid ansvaret for militære efterretninger og overvåger kun civile, når dette er nødvendigt for at varetage agenturets militære funktioner. Det kan navnlig kun efterforske militærpersonel, civilansatte i militæret, personer under militær uddannelse, personer i militærreserven eller rekruttjeneste og krigsfanger (artikel 1 i lov om militærdomstolen). Når forsvarssikkerhedskommandoen indsamler kommunikationsdata til nationale sikkerhedsformål, er den underlagt de begrænsninger og garantier, der er fastsat i CPPA og gennemførelsesdekretet hertil.

([321]) NIS har mandat at indsamle, kompilere og formidle oplysninger om andre lande (dvs. generelle oplysninger om tendenser og udviklingen i forhold til andre lande eller statslige aktørers aktiviteter), efterretninger vedrørende bekæmpelse af spionage (herunder militær og industriel spionage), terrorisme og internationale kriminelle syndikaters aktiviteter, efterretninger om visse former for kriminalitet rettet mod den offentlige og nationale sikkerhed (f.eks. indenlandsk oprør, aggression udefra) og efterretninger i forbindelse med opgaven med at garantere internetsikkerheden og forebygge eller bekæmpe cyberangreb og -trusler (artikel 4, stk. 2, i NIS-loven). Se også bilag II, afsnit 3.1.

overholde relevante retlige krav (herunder PIPA og CPPA) ([322]) og generelle retningslinjer udarbejdet af præsidenten og gennemgået af nationalforsamlingen ([323]). NIS skal som et generelt princip være politisk neutral og beskytte personers friheder og rettigheder ([324]). NIS-medarbejdere må desuden ikke misbruge deres offentlige myndighedsbeføjelser til at tvinge nogen institution, organisation eller enkeltperson til at gøre noget, som de ikke er forpligtet til (ved lov), eller hindre en person i at udøve sine rettigheder ([325]).

3.3.1.1. Adgang til kommunikationsdata

(187) På grundlag af CPPA kan de koreanske offentlige myndigheder ([326]) indsamle kommunikationsbekræftelsesdata (dvs. oplysninger om telekommunikationsdato, start- og sluttidspunkt, antal udgående og indgående opkald samt den anden parts abonnentnummer, hyppighed, logfiler om brugen af teletjenester og lokaliseringsdata, jf. betragtning 155) og indholdet af kommunikation (ved brug af kommunikationsbegrænsende foranstaltninger, jf. betragtning 155) til nationale sikkerhedsformål (som fastsat i NIS-mandatet, jf. fodnote 322 ovenfor). Disse beføjelser omfatter to typer oplysninger: 1) kommunikation, hvor den ene eller begge parter er koreanske statsborgere ([327]), og 2) kommunikation fra a) lande, der er fjendtligt indstillet over for Republikken Korea, b) udenlandske organer, grupper eller statsborgere, der mistænkes for at deltage i antikoreanske aktiviteter ([328]), eller c) medlemmer af grupper, der opererer på Den Koreanske Halvø, men reelt uden at være underlagt Republikken Koreas suverænitet, og deres paraplygrupper i andre lande ([329]). Kommunikation fra EU-borgere, der overføres fra Unionen til Republikken Korea på grundlag af denne afgørelse, kan derfor kun indsamles i henhold til CPPA til nationale sikkerhedsformål (under iagttagelse af de betingelser, der er fastsat i betragtning 188-192), hvis der er tale om kommunikation mellem en EU-borger og en koreansk statsborger, hvis der udelukkende er tale om kommunikation mellem ikkekoreanske statsborgere, eller hvis den falder ind under en af de tre nævnte kategorier 2a), b) og c).

(188) I begge scenarier kan indsamling af kommunikationsbekræftelsesdata kun finde sted for at forebygge trusler mod den nationale sikkerhed ([330]), og der kan kun træffes kommunikationsbegrænsende foranstaltninger, hvis der er en alvorlig risiko for den nationale sikkerhed, og indsamlingen er nødvendig for at forebygge den ([331]). Desuden må der kun gives adgang til indholdet af kommunikation som en sidste udvej, og der skal gøres en indsats for at minimere krænkelsen af privatlivets fred i forbindelse med kommunikation ([332]) og dermed sikre, at det står i et rimeligt forhold til det tilstræbte nationale sikkerhedsmål. Både kommunikationsindhold og kommunikationsbekræftelsesdata kan højst indsamles i fire måneder, og indsamlingen skal straks bringes til ophør, hvis det forfulgte mål nås tidligere ([333]). Hvis de relevante betingelser fortsat er opfyldt, kan fristen forlænges med op til fire måneder med forudgående tilladelse fra en domstol (for de foranstaltninger, der er beskrevet i betragtning 189) eller fra præsidenten (for de foranstaltninger, der er beskrevet i betragtning 190) ([334]).

(189) De samme proceduremæssige garantier gælder for indsamling af kommunikationsbekræftelsesdata og indholdet af kommunikation ([335]). Hvis mindst en af parterne i kommunikationen er koreansk statsborger, skal efterretningsagenturet navnlig indgive en skriftlig anmodning til den højere anklagemyndighed (anklagemyndigheden ved High

([322]) Jf. også artikel 14, 22 og 23 i NIS-loven.
([323]) Jf. artikel 4, stk. 2, i NIS-loven.
([324]) Artikel 3, stk. 1, artikel 6, stk. 2, artikel 11 og 21 i NIS-loven. Se også reglerne om interessekonflikter, navnlig artikel 10 og 12 i NIS-loven.
([325]) Artikel 13 i NIS-loven.
([326]) Dette omfatter efterretningsagenturerne (dvs. NIS og forsvarssikkerhedskommandoen) og politiet/anklagemyndigheden.
([327]) Artikel 7, stk. 1, nr. 1, i CPPA.
([328]) Som forklaret af den koreanske regering i fodnote 244 i bilag II forstås herved aktiviteter, der truer landets eksistens og sikkerhed, den demokratiske orden eller folkets overlevelse og frihed.
([329]) Artikel 7, stk. 1, nr. 2, i CPPA.
([330]) Artikel 13-4 i CPPA.
([331]) Artikel 7, stk. 1, i CPPA.
([332]) Artikel 3, stk. 2, i CPPA. Desuden skal kommunikationsbegrænsende foranstaltninger straks bringes til ophør, når de ikke længere er nødvendige, hvorved det sikres, at enhver krænkelse af den enkeltes ret til kommunikationshemmelighed begrænses til et minimum (artikel 2 i CPPA-gennemførelsesdekretet).
([333]) Artikel 7, stk. 2, i CPPA.
([334]) Anmodningen om godkendelse til at forlænge overvågningsforanstaltningerne skal indgives skriftligt med angivelse af begrundelsen for anmodningen om forlængelse, og der skal vedlægges dokumentation (artikel 7, stk. 2, i CPPA og artikel 5 i CPPA-gennemførelsesdekretet).
([335]) Jf. artikel 13-4, stk. 2, i CPPA og artikel 37, stk. 4, i CPPA-gennemførelsesdekretet, hvori det fastsættes, at de procedurer, der gælder for indsamling af indholdet af kommunikation, finder tilsvarende anvendelse på indsamling af kommunikationsbekræftelsesdata. Se også bilag II, afsnit 3.2.1.1.1.

Court), som derefter skal anmode en retspræsident ved High Court om at udstede en kendelse ([336]). I CPPA anføres de oplysninger, der skal angives i anmodningen til anklageren, anmodningen om kendelsen og selve kendelsen, herunder navnlig om begrundelsen for anmodningen og de vigtigste grunde til mistanke, dokumentation samt oplysninger om formål, mål (dvs. den eller de overvågede personer), omfang og varighed af den foreslåede foranstaltning ([337]). Indsamling må kun finde sted uden en kendelse, hvis der er en sammensværgelse, som truer den nationale sikkerhed, og der foreligger en nødsituation, som gør det umuligt at gennemføre ovennævnte procedurer ([338]). I så fald skal en anmodning om en kendelse imidlertid også indgives umiddelbart efter, at foranstaltningen er truffet ([339]). CPPA definerer derfor klart omfanget af og betingelserne for disse typer indsamling og underkaster dem specifikke (proceduremæssige) garantier (herunder forudgående retslig godkendelse), som sikrer, at anvendelsen af sådanne foranstaltninger er begrænset til, hvad der er nødvendigt og forholdsmæssigt. Desuden udelukker kravet om, at der skal gives detaljerede oplysninger i både anmodningen om en kendelse og selve kendelsen, muligheden for vilkårlig adgang.

(190) For så vidt angår kommunikation mellem ikkekoreanske statsborgere, der falder ind under en af de tre specifikke kategorier anført i betragtning 187, skal der indgives en anmodning til chefen for NIS, som efter en vurdering af hensigtsmæssigheden af de foreslåede foranstaltninger skal anmode Republikken Koreas præsident om en forudgående skriftlig godkendelse ([340]). Den anmodning, der udarbejdes af efterretningsagenturet, skal indeholde de samme detaljerede oplysninger som en anmodning om en retskendelse (jf. betragtning 189), navnlig om begrundelsen for anmodningen og de vigtigste grunde til mistanke, dokumentation og oplysninger om formål, den eller de overvågede personer, omfang og varighed af de foreslåede foranstaltninger ([341]). I nødsituationer ([342]) skal der indhentes forudgående godkendelse fra den minister, som det relevante efterretningsagentur er underlagt, men efterretningsagenturet skal anmode om præsidentens godkendelse umiddelbart efter iværksættelsen af hasteforanstaltningerne ([343]). Hvis der udelukkende er tale om indsamling af kommunikation mellem ikkekoreanske statsborgere, begrænser CPPA derfor anvendelsen af sådanne foranstaltninger til, hvad der er nødvendigt og forholdsmæssigt, ved klart at afgrænse de begrænsede kategorier af personer, der kan være omfattet af sådanne foranstaltninger, og ved at fastsætte detaljerede kriterier, som efterretningsagenturerne skal påvise, at de opfylder, for at begrunde anmodningen om indsamling af oplysninger. Dette udelukker ligeledes muligheden for vilkårlig adgang. Selv om der ikke er nogen forudgående uafhængig godkendelse af sådanne foranstaltninger, fører navnlig PIPC og NHRC et efterfølgende uafhængigt tilsyn (jf. f.eks. betragtning 199-200).

(191) CPPA indfører desuden en række yderligere garantier, der bidrager til efterfølgende tilsyn og letter berørte personers adgang til effektive retsmidler. For det første fastsætter CPPA forskellige registrerings- og rapporteringskrav i forbindelse med enhver form for indsamling til nationale sikkerhedsformål. Efterretningsagenturer, der anmoder private operatører om at samarbejde, skal navnlig indhente en retskendelse eller en tilladelse fra præsidenten eller en kopi af forsiden af en erklæring om censur i nødsituationer, som den pågældende enhed skal opbevare ([344]). Hvis private operatører er tvunget til at samarbejde, skal både den anmodende offentlige myndighed og den pågældende operatør føre fortegnelser over formålet med og genstanden for foranstaltningerne

([336]) Artikel 6, stk. 5 og 8, artikel 7, stk. 1, nr. 1, og artikel 7, stk. 3, i CPPA sammenholdt med artikel 7, stk. 3-4, i CPPA-gennemførelsesdekretet.

([337]) Jf. artikel 7, stk. 3, og artikel 6, stk. 4, i CPPA (vedrørende efterretningsagenturets anmodning), artikel 4 i CPPA-gennemførelsesdekretet (vedrørende anklagerens anmodning) og artikel 7, stk. 3, og artikel 6, stk. 6, i CPPA (vedrørende kendelsen).

([338]) Artikel 8 i CPPA.

([339]) Artikel 8, stk. 2 og 8, i CPPA. Indsamlingen skal straks indstilles, hvis retskendelsen ikke opnås senest 36 timer efter iværksættelsen af foranstaltningerne. Hvis overvågningen afsluttes inden for kort tid og uden en retskendelse, skal chefen for den kompetente højere anklagemyndighed sende en meddelelse om hasteforanstaltninger udarbejdet af efterretningsagenturet til præsidenten for den kompetente domstol, som på dette grundlag kan undersøge, om indsamlingen var lovlig (artikel 8, stk. 5, og 7, i CPPA). I denne meddelelse angives formål, mål, omfang, varighed, gennemførelsessted og overvågningsmetode samt begrundelsen for ikke at indgive en anmodning, inden foranstaltningen træffes (artikel 8, stk. 6, i CPPA). Mere generelt må efterretningsagenturer kun træffe hasteforanstaltninger i overensstemmelse med en »erklæring om censur/aflytning i nødsituationer«, og de skal føre et register over sådanne foranstaltninger (artikel 8, stk. 4, i CPPA).

([340]) Artikel 8, stk. 1 og 2, i CPPA-gennemførelsesdekretet.

([341]) Artikel 8, stk. 3, i CPPA sammenholdt med artikel 6, stk. 4, i CPPA.

([342]) Hvis foranstaltningen er rettet mod en sammensværgelse, der truer den nationale sikkerhed, og der ikke er tilstrækkelig tid til at indhente præsidentens godkendelse og manglende vedtagelse af hasteforanstaltninger kan være til skade for den nationale sikkerhed (artikel 8, stk. 8, i CPPA).

([343]) Artikel 8, stk. 9, i CPPA. Indsamlingen skal straks indstilles, hvis tilladelsen ikke opnås senest 36 timer efter indgivelsen af anmodningen.

([344]) Artikel 9, stk. 2, i CPPA og artikel 12 i CPPA-gennemførelsesdekretet. Jf. artikel 13 i CPPA-gennemførelsesdekretet om muligheden for at kræve bistand fra postkontorer og teleudbydere. Private operatører, der anmodes om at videregive oplysninger, kan nægte at gøre dette, hvis der i kendelsen/tilladelsen eller erklæringen om censur i nødsituationer angives en forkert identifikator (f.eks. et telefonnummer tilhørende en anden person end den identificerede person). De må under alle omstændigheder ikke videregive adgangskoder, der anvendes til kommunikation (artikel 9, stk. 4, i CPPA).

samt datoen for gennemførelsen ([345]). Desuden skal efterretningsagenturerne aflægge rapport om de oplysninger, de har indsamlet, og om resultaterne af overvågningen til chefen for NIS ([346]).

(192) For det andet skal de berørte personer underrettes om indsamlingen af deres oplysninger (kommunikationsbekræftelsesdata eller indholdet af kommunikation) til nationale sikkerhedsformål, hvis mindst en af parterne i kommunikationen er koreansk statsborger ([347]). Denne underretning skal ske skriftligt senest 30 dage efter den dato, hvor indsamlingen blev afsluttet (herunder hvis oplysningerne blev indsamlet efter hasteproceduren), og må kun udsættes, hvis og så længe den bringer den nationale sikkerhed i fare eller er til skade for menneskers liv og fysiske sikkerhed ([348]). Uanset denne underretning har de berørte personer adgang til forskellige prøvelsesmekanismer som nærmere forklaret i afsnit 3.3.4.

3.3.1.2. Indsamling af oplysninger om terrormistænkte

(193) I henhold til antiterrorloven kan NIS indsamle oplysninger om terrormistænkte ([349]) i overensstemmelse med de begrænsninger og garantier, der er fastsat i andre love ([350]). NIS kan navnlig indhente kommunikationsdata (på grundlag af CPPA) og andre personoplysninger (gennem en anmodning om frivillig fremlæggelse af oplysninger ([351])). Med hensyn til indsamling af kommunikationsdata (dvs. indholdet af kommunikation eller kommunikationsbekræftelsesdata) finder de begrænsninger og garantier, der er beskrevet i afsnit 3.3.1.1, anvendelse, herunder kravet om at indhente en retskendelse. Med hensyn til anmodninger om frivillig fremlæggelse af andre typer personoplysninger om terrormistænkte skal NIS overholde kravene i forfatningen og PIPA om nødvendighed og proportionalitet (jf. betragtning 164) ([352]). Dataansvarlige, der modtager sådanne anmodninger, kan imødekomme dem frivilligt på de betingelser, der er fastsat i PIPA (f.eks. i overensstemmelse med princippet om dataminimering og ved at begrænse indvirkningen på den enkeltes ret til privatlivets fred) ([353]). I så fald skal de også opfylde kravet om at underrette den berørte person i henhold til meddelelse nr. 2021-5 (jf. betragtning 166).

([345]) Med hensyn til kommunikationsbegrænsende foranstaltninger skal sådanne fortegnelser opbevares i tre år, jf. artikel 9, stk. 3, i CPPA og artikel 17, stk. 2, i CPPA-gennemførelsesdekretet. Med hensyn til kommunikationsbekræftelsesdata skal efterretningsagenturerne føre fortegnelser over, at der er indgivet en anmodning om sådanne oplysninger, og over selve den skriftlige anmodning og den institution, der har indgivet den (artikel 13, stk. 5, og artikel 13-4, stk. 3, i CPPA). Teleudbydere skal opbevare fortegnelser i syv år og to gange om året aflægge rapport til ministeren for videnskab og IKT om hyppigheden af denne videregivelse (artikel 9, stk. 3, i CPPA sammenholdt med artikel 13, stk. 7, i CPPA og artikel 37, stk. 4, og artikel 39 i CPPA-gennemførelsesdekretet).

([346]) Artikel 18, stk. 3, i CPPA-gennemførelsesdekretet.

([347]) Artikel 9-2, stk. 3, og artikel 13-4 i CPPA. Underretningen skal indeholde 1) en angivelse af, at oplysningerne er indsamlet, 2) gennemførelsesmyndigheden og 3) gennemførelsesperioden.

([348]) Artikel 9-2, stk. 4, i CPPA. I så fald skal underretningen ske senest 30 dage efter, at årsagerne til udsættelsen ikke længere gør sig gældende, jf. artikel 13-4, stk. 2, og artikel 9-2, stk. 6, i CPPA.

([349]) Medlemmer af en terrorgruppe (opført på FN's liste, jf. artikel 2, stk. 2, i antiterrorloven), personer, der fremmer og udbreder en terrorgruppes idéer eller taktikker, rejser eller bidrager til finansiering af terrorisme eller deltager i andre aktiviteter såsom forberedelse, sammensværgelse, udbredelse af propaganda om eller anstiftelse af terrorisme, eller personer, hvor der er begrundet mistanke om, at de har udført sådanne aktiviteter (artikel 2, stk. 3, i antiterrorloven). »Terrorisme« defineres i artikel 2, stk. 1, i antiterrorloven som handlinger, der udføres med det formål at hindre statens, en lokal myndigheds eller en udenlandsk regerings myndighedsudøvelse (herunder internationale organisationer) eller med det formål at tvinge dem til at handle uden nogen retlig forpligtelse hertil eller true offentligheden. Sådanne handlinger kan f.eks. omfatte drab, kidnapning eller gidseltagning, kapring/beslaglæggelse, ødelæggelse eller beskadigelse af et skib eller luftfartøj, anvendelse af biokemiske, eksplosive eller brændbare våben med det formål at forårsage død, alvorlig tilskadekomst eller skade og misbrug af nukleare eller radioaktive materialer.

([350]) Artikel 9, stk. 1 og 3, i antiterrorloven.

([351]) I antiterrorloven henvises også til muligheden for at indsamle oplysninger om indrejse i og udrejse fra Republikken Korea på grundlag af immigrationsloven og toldloven, men disse love indeholder i øjeblikket ikke en sådan bemyndigelse (jf. afsnit 3.2.2.1 i bilag II). Under alle omstændigheder vil de i princippet ikke finde anvendelse på oplysninger, der overføres på grundlag af denne afgørelse, da de typisk vedrører oplysninger, der indsamles direkte af de koreanske myndigheder (og ikke adgang til oplysninger, der tidligere er overført fra Unionen til koreanske dataansvarlige). Desuden henvises der i antiterrorloven til ARUSFTI som retsgrundlag for indsamling af oplysninger om finansielle transaktioner. Som forklaret i fodnote 200 falder de typer oplysninger, der kan indhentes på grundlag af denne lov, imidlertid ikke ind under denne afgørelses anvendelsesområde. Endelig kan NIS i henhold til antiterrorloven også indsamle lokaliseringsdata gennem ikkebindende anmodninger, hvor udbydere af lokaliseringsdata frivilligt kan videregive sådanne oplysninger på de betingelser, der er fastsat i PIPA (jf. betragtning 193) og i lov om lokaliseringsdata. Som også forklaret i fodnote 17 vil lokaliseringsdata imidlertid ikke blive overført fra Unionen til koreanske dataansvarlige på grundlag af denne afgørelse, idet de vil blive frembragt i Korea.

([352]) Jf. bilag II, afsnit 3.2.2.2.

([353]) Jf. artikel 58, stk. 4, i PIPA, som fastsætter, at personoplysninger skal behandles i mindst muligt omfang for at nå det tilsigtede formål, og artikel 3, stk. 6, i PIPA, som fastsætter, at personoplysninger skal behandles på en måde, der minimerer risikoen for at krænke den enkeltes ret til privatlivets fred. Se også artikel 59, nr. 2 og 3, i PIPA, hvori det fastsættes, at dataansvarlige ikke må videregive personoplysninger til tredjemand uden tilladelse.

3.3.1.3. Anmodninger om frivillig fremlæggelse af oplysninger af abonnentdata

(194) Teleudbydere kan frivilligt videregive abonnentoplysninger på grundlag af TBA (jf. betragtning 163) efter anmodning fra et efterretningsagentur, der agter at indsamle sådanne oplysninger for at forebygge en trussel mod den nationale sikkerhed ([354]). For sådanne anmodninger fra NIS gælder de samme begrænsninger (som følger af forfatningen, PIPA og TBA) som inden for strafferetlig håndhævelse, jf. betragtning 164 ([355]). Teleudbydere er ikke forpligtet til at imødekommer sådanne anmodninger og kan kun gøre dette på de betingelser, der er fastsat i PIPA (navnlig i overensstemmelse med princippet om dataminimering og ved at begrænse indvirkningen på den enkeltes ret til privatlivets fred, se også betragtning 193). Der gælder samme krav med hensyn til registrering og underretning af den pågældende person som inden for strafferetlig håndhævelse (jf. betragtning165 og 166).

3.3.2. *Yderligere anvendelse af de indsamlede oplysninger*

(195) Behandlingen af personoplysninger, der indsamles af de koreanske myndigheder til nationale sikkerhedsformål, er underlagt principperne om formålsbegrænsning (artikel 3, stk. 1 og 2, i PIPA), lovlig og rimelig behandling (artikel 3, stk. 1, i PIPA), proportionalitet/dataminimering (artikel 3, stk. 1 og 6, og artikel 58 i PIPA), nøjagtighed (artikel 3, stk. 3, i PIPA), gennemsigtighed (artikel 3, stk. 5, i PIPA), sikkerhed (artikel 58, stk. 4, i PIPA) og opbevaringsbegrænsning (artikel 58, stk. 4, i PIPA) ([356]). Eventuel videregivelse af personoplysninger til tredjemand (herunder tredjelande) kan kun finde sted i overensstemmelse med disse principper (navnlig om formålsbegrænsning og dataminimering) efter en vurdering af overholdelsen af principperne om nødvendighed og proportionalitet (forfatningens artikel 37, stk. 2) og under hensyntagen til indvirkningen på de berørte personers rettigheder (artikel 3, stk. 6, i PIPA).

(196) Hvad angår indholdet af kommunikation og kommunikationsbekræftelsesdata begrænser CPPA yderligere anvendelsen af sådanne oplysninger til retssager, hvor en part i kommunikationen påberåber sig disse i et erstatningssøgsmål, eller til tilladte anvendelser i henhold til anden lovgivning ([357]).

3.3.3. *Tilsyn*

(197) De koreanske nationale sikkerhedsmyndigheders aktiviteter overvåges af forskellige organer ([358]).

(198) For det første indeholder antiterrorloven bestemmelser om specifikke tilsynsmekanismer for terrorbekæmpelsesaktiviteter, herunder indsamling af oplysninger om terrormistænkte. Navnlig på det udøvende niveau overvåges terrorbekæmpelsesaktiviteter af antiterrorkommissionen ([359]), som chefen for NIS skal aflægge rapport til om efterforskning og sporing af terrormistænkte for at indsamle de nødvendige oplysninger eller materialer til terrorbekæmpelsesaktiviteter ([360]). Den ansvarlige for beskyttelse af menneskerettigheder (HRPO) fører desuden specifikt tilsyn med, at terrorbekæmpelsesaktiviteterne ikke krænker de grundlæggende rettigheder ([361]). HRPO udnævnes af formanden for antiterrorkommissionen blandt personer, der opfylder specifikke kvalifikationskriterier anført i gennemførelsesdekretet til antiterrorloven ([362]), for en periode på to år, som kan forlænges, og kan kun afsættes af specifikke, begrænsede grunde, og hvis det er berettiget ([363]). Under udøvelsen af sin

([354]) Artikel 83, stk. 3, i TBA.
([355]) Se også bilag II, afsnit 3.2.3.
([356]) Jf. bilag II, afsnit 1.2.
([357]) Artikel 5, stk. 1-2, artikel 12 og 13-5 i CPPA.
([358]) Jf. bilag II, afsnit 3.3.
([359]) Artikel 5, stk. 3, i antiterrorloven. Kommissionen ledes af premierministeren og består af flere ministre og myndighedschefer, herunder udenrigsministeren, justitsministeren, forsvarsministeren, indenrigs- og sikkerhedsministeren, chefen for NIS og generalkommissæren for det nationale politiagentur (artikel 3, stk. 1, i gennemførelsesdekretet til antiterrorloven).
([360]) Artikel 9, stk. 4, i antiterrorloven.
([361]) Artikel 7 i antiterrorloven.
([362]) Enhver, der har udøvet hvervet som advokat, med mindst ti års erhvervserfaring eller med ekspertviden på menneskerettighedsområdet, og som arbejder eller har arbejdet (som minimum) på lektorniveau i mindst ti år eller har bestridt en højere embedsmandsstilling i statsforvaltninger eller lokale myndigheder eller med mindst ti års erhvervserfaring på menneskerettighedsområdet, f.eks. i en ikkestatslig organisation (artikel 7, stk. 1, i gennemførelsesdekretet til antiterrorloven).
([363]) F.eks. når der er rejst tiltale i en straffesag vedrørende vedkommendes opgaver, i forbindelse med videregivelse af fortrolige oplysninger eller på grund af langvarig psykisk eller fysisk sygdom (artikel 7, stk. 3, i antiterrorloven).

tilsynsfunktion kan HRPO udstede generelle henstillinger om forbedringer af beskyttelsen af menneskerettighederne ([364]) og specifikke henstillinger om korrigerende foranstaltninger, hvis der er konstateret en krænkelse af menneskerettighederne ([365]). De offentlige myndigheder skal underrette HRPO'en om opfølgningen på dens henstillinger ([366]).

(199) For det andet fører PIPC tilsyn med, at de nationale sikkerhedsmyndigheder overholder databeskyttelsesreglerne, hvilket omfatter både de gældende bestemmelser i PIPA (jf. betragtning 149) og de begrænsninger og garantier, der gælder for indsamling af personoplysninger i henhold til andre love (CPPA, antiterrorloven og TBA, se også betragtning 171) ([367]). Ved udøvelsen af denne tilsynsrolle kan PIPC gøre brug af alle sine undersøgelsesbeføjelser og afhjælpende beføjelser som nærmere beskrevet i afsnit 2.4.2.

(200) For det tredje er de nationale sikkerhedsmyndigheders aktiviteter underlagt NHRC's uafhængige tilsyn i overensstemmelse med de procedurer, der er beskrevet i betragtning 172 ([368]).

(201) For det fjerde omfatter BAI's tilsynsfunktion også de nationale sikkerhedsmyndigheder, selv om NIS under ekstraordinære omstændigheder kan nægte at udlevere visse oplysninger eller materialer, f.eks. hvis de udgør statshemmeligheder, og offentlighedens kendskab hertil ville have en alvorlig indvirkning på den nationale sikkerhed ([369]).

(202) Endelig varetages den parlamentariske kontrol med NIS' aktiviteter af nationalforsamlingen (gennem et specialiseret efterretningsudvalg) ([370]). Nationalforsamlingens særlige kontrolfunktion med hensyn til anvendelsen af kommunikationsbegrænsende foranstaltninger til nationale sikkerhedsformål er fastsat i CPPA ([371]). Nationalforsamlingen kan navnlig foretage inspektion på stedet af aflytningsudstyr og kan kræve, at både NIS og teleoperatører, der har offentliggjort indholdet af kommunikation, aflægger rapport herom. Nationalforsamlingen kan også udføre sine generelle kontrolfunktioner (i overensstemmelse med de procedurer, der er beskrevet i betragtning 174). I henhold til NIS-loven skal chefen for NIS reagere straks, når efterretningsudvalget anmoder om en rapport om et specifikt spørgsmål ([372]), og der er specifikke regler for visse særligt følsomme oplysninger. Helt konkret kan chefen for NIS kun nægte at svare eller afgive vidneforklaring i udvalget under ekstraordinære omstændigheder, dvs. hvis anmodningen vedrører statshemmeligheder om militære, diplomatiske eller nordkoreanske spørgsmål, hvor offentlighedens kendskab kan have en alvorlig indvirkning på landets »nationale skæbne« ([373]). I så fald kan efterretningsudvalget anmode premierministeren om en forklaring, og hvis der ikke gives en forklaring inden for syv dage, kan svaret eller vidneforklaringer ikke afslås.

3.3.4. *Klageadgang*

(203) I det koreanske system er der også forskellige (retlige) klagemuligheder på det nationale sikkerhedsområde, herunder mulighed for at opnå skadeserstatning. Disse mekanismer giver de registrerede adgang til effektive administrative og retlige klagemuligheder, der navnlig sætter dem i stand til at håndhæve deres rettigheder, herunder retten til at få adgang til deres personoplysninger eller til at få sådanne oplysninger berigtiget eller slettet.

(204) For det første kan enkeltpersoner i henhold til artikel 3, stk. 5, og artikel 4, stk. 1, 3 og 4, i PIPA udøve deres ret til indsigt, berigtigelse, sletning og suspension over for de nationale sikkerhedsmyndigheder. I afsnit 6 i meddelelse nr. 2021-5 (bilag I til denne afgørelse) præciseres det yderligere, hvordan disse rettigheder finder anvendelse i forbindelse med databehandling til nationale sikkerhedsformål. En national sikkerhedsmyndighed kan navnlig kun begrænse eller nægte udøvelsen af en sådan rettighed, i det omfang og så længe det er nødvendigt og forholdsmæssigt for at beskytte et vigtigt mål af samfundsmæssig interesse (f.eks. i det omfang og så længe indrømmelsen

([364]) Artikel 8, stk. 1, i gennemførelsesdekretet til antiterrorloven.
([365]) Artikel 9, stk. 1, i gennemførelsesdekretet til antiterrorloven. HRPO træffer selv afgørelse om vedtagelsen af henstillinger, men skal rapportere sådanne henstillinger til formanden for antiterrorkommissionen.
([366]) Artikel 9, stk. 2, i gennemførelsesdekretet til antiterrorloven. Ifølge den koreanske regerings officielle repræsentation vil manglende gennemførelse af en henstilling fra HRPO blive forelagt antiterrorkommissionen, herunder premierministeren, selv om der hidtil ikke har været tilfælde, hvor henstillingerne fra HRPO ikke er blevet gennemført (jf. afsnit 3.3.1 i bilag II).
([367]) Bilag II, afsnit 3.3.4.
([368]) Med hensyn til NIS har NHRC tidligere foretaget undersøgelser på eget initiativ og behandlet en række individuelle klager. Jf. f.eks. NHRC's årsrapport for 2018, s. 128 (findes på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7604746) og NHRC's årsrapport for 2019, s. 70 (findes på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([369]) Jf. artikel 13, stk. 1, i NIS-loven.
([370]) Jf. artikel 36 og artikel 37, stk. 1, 15, i lov om nationalforsamlingen.
([371]) Artikel 15 i CPPA.
([372]) Jf. artikel 15, stk. 2, i NIS-loven.
([373]) Jf. artikel 17, stk. 2, i NIS-loven. »Statshemmeligheder« defineres som (klassificerede) kendsgerninger, varer eller viden, som ikke må videregives til andre lande eller organisationer for at undgå alvorlige indvirkninger på den nationale sikkerhed, og hvortil der kun er begrænset adgang. Jf. artikel 13, stk. 4, i NIS-loven.

af rettigheden vil bringe en igangværende efterforskning i fare eller true den nationale sikkerhed), eller hvis indrømmelsen af rettigheden kan skade tredjemands liv eller legeme. Påberåbelse af en sådan begrænsning kræver således en afvejning af den enkeltes rettigheder og interesser i forhold til den relevante offentlige interesse og må ikke berøre rettighedens væsentligste indhold (forfatningens artikel 37, stk. 2). Hvis anmodningen afslås eller begrænses, skal den pågældende straks underrettes om årsagerne hertil.

(205) For det andet har personer adgang til prøvelse i henhold til PIPA, hvis deres oplysninger er blevet behandlet af en national sikkerhedsmyndighed i strid med PIPA eller begrænsningerne og garantierne i anden lovgivning om indsamling af personoplysninger (navnlig CPPA, jf. betragtning 171) ([374]). Denne ret kan udøves ved at indgive en klage til PIPC (herunder via callcentret for privatlivsbeskyttelse, der drives af Koreas internet- og sikkerhedsagentur) ([375]). For at lette adgangen til at klage over koreanske nationale sikkerhedsmyndigheder kan EU-borgere desuden indgive en klage til PIPC via deres nationale databeskyttelsesmyndighed ([376]). I så fald underretter PIPC den pågældende via den nationale databeskyttelsesmyndighed, når undersøgelsen er afsluttet (herunder, hvis det er relevant, med oplysninger om de pålagte korrigerende foranstaltninger). På grundlag af lov om forvaltningssager kan enkeltpersoner desuden påklage/anfægte PIPC's afgørelser eller manglende handling (jf. betragtning 132).

(206) For det tredje kan enkeltpersoner indgive en klage til HRPO om krænkelse af deres ret til privatlivets fred/databeskyttelse i forbindelse med terrorbekæmpelsesaktiviteter (dvs. i henhold til antiterrorloven) ([377]), som kan henstille, at der træffes korrigerende foranstaltninger. Da der ikke stilles krav om antagelighed ved indgivelse af en klage til HRPO, vil en klage blive behandlet, selv om den pågældende person ikke kan påvise, at vedkommende rent faktisk har lidt skade (f.eks. på grund af en national sikkerhedsmyndigheds påståede ulovlige indsamling af vedkommendes oplysninger) ([378]). Den relevante myndighed skal underrette HRPO'en om de foranstaltninger, der træffes for at gennemføre dens henstillinger.

(207) For det fjerde kan personer indgive en klage til NHRC vedrørende de nationale sikkerhedsmyndigheders indsamling af deres oplysninger og få prøvet deres sag i overensstemmelse med den procedure, der er beskrevet i betragtning 178 ([379]).

(208) Endelig findes der forskellige retsmidler ([380]), som giver enkeltpersoner mulighed for at påberåbe sig de begrænsninger og garantier, der er beskrevet i afsnit 3.3.1, ved at få prøvet deres sag domstolene. Enkeltpersoner kan navnlig anfægte lovligheden af de nationale sikkerhedsmyndigheders handlinger på grundlag af lov om forvaltningssager (i overensstemmelse med den procedure, der er beskrevet i betragtning 181 eller i lov om forfatningsdomstolen (jf. betragtning 182). De har derudover mulighed for at opnå skadeserstatning på grundlag af lov om erstatning fra staten (som nærmere beskrevet i betragtning 183).

4. **KONKLUSION**

(209) Kommissionen finder, at Republikken Korea — gennem PIPA, de særlige regler, der gælder for visse sektorer (som analyseret i afsnit 2) og de supplerende garantier i meddelelse nr. 2021-5 (bilag I) — sikrer et beskyttelsesniveau for personoplysninger overført fra Den Europæiske Union, som i det væsentlige svarer til det niveau, der er garanteret ved forordning (EU) 2016/679.

(210) Kommissionen finder desuden ud fra en samlet betragtning, at tilsyns- og prøvelsesmekanismerne i koreansk ret i praksis gør det muligt at identificere og sanktionere overtrædelser af databeskyttelsesreglerne begået af dataansvarlige i Korea, og at de sikrer den registrerede retsmidler til at få adgang til personoplysninger, som vedrører pågældende, og til efterfølgende at få sådanne oplysninger berigtiget eller slettet.

([374]) Artikel 58, stk. 4, og artikel 4, stk. 5, i PIPA. Jf. bilag II, afsnit 3.4.2.
([375]) Artikel 62 og artikel 63, stk. 2, i PIPA.
([376]) Meddelelse nr. 2021-5 (afsnit 6, bilag I).
([377]) Artikel 8, stk. 1, nr. 2, i gennemførelsesdekretet til antiterrorloven.
([378]) Jf. bilag II, afsnit 3.4.1.
([379]) F.eks. modtager NHRC regelmæssigt klager over den nationale efterretningstjeneste, se tallene i NHRC's årsrapport for 2019 om antallet af modtagne klager mellem 2015 og 2019, s. 70 (findes på https://www.humanrights.go.kr/site/program/board/basicboard/view?menuid=002003003001&pagesize=10&boardtypeid=7017&boardid=7606217).
([380]) Jf. bilag II, afsnit 3.4.4.

(211) Endelig finder Kommissionen på grundlag af de tilgængelige oplysninger om den koreanske retsorden, herunder de i bilag II indeholdte redegørelser, forsikringer og tilsagn fra den koreanske regering, at ethvert indgreb i offentlighedens interesse, navnlig med henblik på strafferetlig håndhævelse og af nationale sikkerhedshensyn, i de grundlæggende rettigheder for enkeltpersoner, hvis personoplysninger overføres fra Den Europæiske Union til Republikken Korea, som foretages af de koreanske myndigheder, vil være begrænset til, hvad der er strengt nødvendigt for at nå det pågældende legitime mål, og at der findes en effektiv retsbeskyttelse mod et sådant indgreb.

(212) I lyset af konklusionerne i denne afgørelse bør det derfor besluttes, at Republikken Korea sikrer et tilstrækkeligt beskyttelsesniveau som omhandlet i artikel 45 i forordning (EU) 2016/679, fortolket i lyset af Den Europæiske Unions charter om grundlæggende rettigheder, for personoplysninger, som overføres fra Den Europæiske Union til Republikken Korea til persondataansvarlige i Republikken Korea, der er omfattet af PIPA, med undtagelse af religiøse organisationer, i det omfang de behandler personoplysninger i forbindelse med deres missionsarbejde, politiske partier, i det omfang de behandler personoplysninger i forbindelse med udnævnelsen af kandidater, og dataansvarlige, der er underlagt kommissionen for finansielle tjenesteydelsers tilsyn med behandlingen af personlige kreditoplysninger i medfør af lov om kreditoplysninger, i det omfang de behandler sådanne oplysninger.

5. VIRKNINGERNE AF DENNE AFGØRELSE OG DATABESKYTTELSESMYNDIGHEDERNES HANDLINGER

(213) Medlemsstaterne og deres organer er forpligtet til at træffe de nødvendige foranstaltninger for at overholde EU-institutionernes retsakter, da der gælder en formodning om, at disse retsakter er lovlige, og de afføder derfor retsvirkninger, så længe de ikke er blevet trukket tilbage, annulleret under et annullationssøgsmål eller erklæret ugyldige som følge af en præjudiciel forelæggelse eller en ulovlighedsindsigelse.

(214) En afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet i henhold til artikel 45, stk. 3, i forordning (EU) 2016/679 er således bindende for alle de organer i medlemsstaterne, som den er rettet til, herunder deres uafhængige tilsynsmyndigheder. Overførsler fra en dataansvarlig eller databehandler i Den Europæiske Union til dataansvarlige i Republikken Korea kan navnlig finde sted, uden at der behøves yderligere tilladelse.

(215) Det bør bemærkes, at i henhold til artikel 58, stk. 5, i forordning (EU) 2016/679, og som Domstolen forklarede i Schrems-dommen ([381]), skal den nationale lovgivning, når en national databeskyttelsesmyndighed, herunder efter en klage, sætter spørgsmålstegn ved, om en afgørelse fra Kommissionen om tilstrækkeligheden af beskyttelsesniveauet er forenelig med den enkeltes grundlæggende ret til privatlivets fred og databeskyttelse, giver den pågældende mulighed for at indbringe disse indsigelser for en national domstol, som kan være forpligtet til at forelægge Domstolen et præjudicielt spørgsmål ([382]).

6. OVERVÅGNING OG REVISION AF DENNE AFGØRELSE

(216) Ifølge Domstolens praksis ([383]) og som anerkendt i artikel 45, stk. 4, i forordning (EU) 2016/679 bør Kommissionen løbende overvåge den relevante udvikling i tredjelandet efter vedtagelsen af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet for at vurdere, hvorvidt tredjelandet stadig sikrer et i det væsentlige tilsvarende beskyttelsesniveau. En sådan undersøgelse skal under alle omstændigheder foretages, når Kommissionen modtager oplysninger, der rejser begrundet tvivl i denne henseende.

(217) Kommissionen bør derfor løbende overvåge situationen i Republikken Korea med hensyn til de retlige rammer og den faktiske praksis i behandlingen af personoplysninger, som er blevet vurderet i denne afgørelse, herunder om de koreanske myndigheder holder sig til de redegørelser, forsikringer og tilsagn, der er indeholdt i bilag II. For at lette denne proces opfordres de koreanske myndigheder til straks at underrette Kommissionen om væsentlige ændringer, som er relevante for denne afgørelse, hvad angår de erhvervsdrivendes og offentlige myndigheders behandling af personoplysninger samt de begrænsninger og garantier, som finder anvendelse for offentlige myndigheders adgang til personoplysninger.

([381]) Schrems, præmis 65.

([382]) Schrems, præmis 65: »I denne henseende påhviler det den nationale lovgiver at tilvejebringe retsmidler, der gør det muligt for den pågældende nationale tilsynsmyndighed at indbringe de klagepunkter, som den finder begrundede, for de nationale domstole, således at disse, såfremt de deler myndighedens tvivl vedrørende gyldigheden af Kommissionens afgørelse, kan foretage en præjudiciel forelæggelse med henblik på en efterprøvelse af denne afgørelses gyldighed.«

([383]) Schrems, præmis 76.

(218) For at gøre det muligt for Kommissionen at udøve sin overvågningsfunktion effektivt bør medlemsstaterne desuden underrette Kommissionen om alle relevante foranstaltninger, der træffes af de nationale databeskyttelsesmyndigheder, navnlig vedrørende forespørgsler eller klager fra registrerede i EU vedrørende overførsel af personoplysninger fra Den Europæiske Union til dataansvarlige i Republikken Korea. Kommissionen bør også underrettes om enhver indikation på, at de koreanske myndigheder med ansvar for forebyggelse, efterforskning, afsløring og retsforfølgelse strafbare handlinger eller for den nationale sikkerhed, herunder alle tilsynsmyndigheder, ikke handler på en måde, der sikrer det krævede beskyttelsesniveau.

(219) I medfør af artikel 45, stk. 3, i forordning (EU) 2016/679 ([384]) og henset til den omstændighed, at det beskyttelsesniveau, som den koreanske retsorden sikrer, kan ændre sig, vil Kommissionen efter vedtagelse af denne afgørelse med regelmæssige mellemrum undersøge, om konstateringen af det tilstrækkelige beskyttelsesniveau, som er sikret af Republikken Korea, stadig er faktisk og retligt begrundet.

(220) Med henblik herpå bør første revision af denne afgørelse foretages tre år efter dens ikrafttræden. Efter den første revision og afhængigt af dennes resultat vil Kommissionen i nært samråd med det udvalg, der er nedsat i henhold til artikel 93, stk. 1, i forordning (EU) 2016/679, beslutte, om den treårige cyklus bør opretholdes. Under alle omstændigheder bør de efterfølgende revisioner finde sted mindst hvert fjerde år ([385]). Revisionen bør omfatte alle aspekter af denne afgørelses funktionsmåde, navnlig anvendelsen af de supplerende garantier i bilag I til denne afgørelse, med særlig opmærksomhed på den beskyttelse, der gives i tilfælde af videreoverførsler, relevant udvikling i retspraksis, reglerne for behandling af pseudonymiserede oplysninger til statistiske formål, videnskabelige forskningsformål og arkivformål i samfundets interesse samt anvendelsen af undtagelserne i artikel 28, stk. 7, i PIPA, effektiviteten af udøvelsen af individuelle rettigheder, herunder for den nyligt reformerede PIPC, og anvendelsen af undtagelser fra disse rettigheder, anvendelsen af de delvise undtagelser i PIPA samt begrænsningerne og garantierne med hensyn til myndighedsadgang (som fastsat i bilag II til denne afgørelse), herunder PIPC's samarbejde med EU's databeskyttelsesmyndigheder om klager fra enkeltpersoner. Den bør også omfatte effektiviteten af tilsyn og håndhævelse, både med hensyn til PIPA og strafferetlig retshåndhævelse og national sikkerhed (navnlig i PIPC- og NHRC-regi).

(221) Med henblik på at foretage revisionen bør Kommissionen mødes med PIPC, som efter behov kan ledsages af andre koreanske myndigheder med ansvar for myndighedsadgang, herunder de relevante tilsynsorganer. Deltagelsen i dette møde bør være åben for repræsentanter for medlemmerne af Det Europæiske Databeskyttelsesråd. Inden for rammerne af revisionen bør Kommissionen anmode PIPC om omfattende oplysninger om alle aspekter, der er relevante for konstateringen af et tilstrækkeligt beskyttelsesniveau, herunder om begrænsningerne og garantierne vedrørende myndigheders adgang ([386]). Kommissionen bør også indhente redegørelser vedrørende eventuelle oplysninger med relevans for denne afgørelse, som den har modtaget, herunder offentlige rapporter fra koreanske myndigheder eller andre interessenter i Korea, Det Europæiske Databeskyttelsesråd, individuelle databeskyttelsesmyndigheder, civilsamfundsgrupper, medierne eller andre tilgængelige informationskilder.

(222) Kommissionen vil på grundlag af revisionen udarbejde en offentlig rapport til Europa-Parlamentet og Rådet.

7. SUSPENSION, OPHÆVELSE ELLER ÆNDRING AF DENNE AFGØRELSE

(223) Hvis tilgængelige oplysninger, navnlig oplysninger fra overvågningen i henhold til denne afgørelse eller fra Koreas eller medlemsstaternes myndigheder, viser, at det beskyttelsesniveau, som Republikken Korea yder, måske ikke længere er tilstrækkeligt, bør Kommissionen straks underrette de kompetente koreanske myndigheder herom og anmode om, at der træffes passende foranstaltninger inden for en nærmere fastsat og rimelig tidsramme.

(224) Hvis Koreas kompetente myndigheder ved udløbet af den fastsatte tidsramme ikke træffer disse foranstaltninger eller på anden måde på tilfredsstillende vis godtgør, at denne afgørelse fortsat er baseret på et passende beskyttelsesniveau, indleder Kommissionen proceduren i artikel 93, stk. 2, i forordning (EU) 2016/679 med henblik på helt eller delvis at suspendere eller ophæve denne afgørelse.

(225) Alternativt vil Kommissionen indlede den pågældende procedure med henblik på at ændre afgørelsen, navnlig ved at underkaste dataoverførsler yderligere betingelser eller ved at begrænse omfanget af konstateringen af et tilstrækkeligt beskyttelsesniveau til kun at omfatte dataoverførsler, for hvilke der fortsat sikres et tilstrækkeligt beskyttelsesniveau.

([384]) Artikel 45, stk. 3, i forordning (EU) 2016/679: »[i] den pågældende gennemførelsesretsakt fastsættes en mekanisme for regelmæssig revision, som foretages (…), og som inddrager enhver relevant udvikling i tredjelandet eller den internationale organisation«.

([385]) Artikel 45, stk. 3, i forordning (EU) 2016/679 foreskriver, at en regelmæssig revision skal finde sted »mindst hvert fjerde år«. Se også Det Europæiske Databeskyttelsesråd, Adequacy Referential, WP 254 rev. 01.

([386]) Jf. bilag II til denne afgørelse.

(226) Kommissionen bør navnlig indlede proceduren for suspension eller ophævelse, hvis der er tegn på, at de yderligere garantier i bilag I ikke overholdes af erhvervsdrivende, der modtager personoplysninger i henhold til denne afgørelse, og/eller ikke håndhæves effektivt, eller at de koreanske myndigheder ikke efterlever de redegørelser, forsikringer og tilsagn, som er indeholdt i bilag II til denne afgørelse.

(227) Kommissionen bør ligeledes overveje at indlede proceduren med henblik på ændring, suspension eller ophævelse af denne afgørelse, hvis de koreanske myndigheder i forbindelse med revisionen eller på anden vis undlader at forelægge de oplysninger og præciseringer, der er nødvendige for at vurdere beskyttelsesniveauet for personoplysninger, der overføres fra Den Europæiske Union til Republikken Korea, eller for at vurdere overholdelsen af denne afgørelse. I den forbindelse bør Kommissionen tage hensyn til, i hvilket omfang de relevante oplysninger kan indhentes fra andre kilder.

(228) I behørigt begrundede særligt hastende tilfælde vil Kommissionen gøre brug af muligheden for efter proceduren i artikel 93, stk. 3, i forordning (EU) 2016/679 at vedtage gennemførelsesretsakter, der finder anvendelse straks, og som suspenderer, ophæver eller ændrer afgørelsen.

8. **AFSLUTTENDE BETRAGTNINGER**

(229) Det Europæiske Databeskyttelsesråd har offentliggjort sin udtalelse ([387]), som er blevet taget i betragtning ved udarbejdelsen af denne afgørelse.

(230) Foranstaltningerne i denne afgørelse er i overensstemmelse med udtalelsen fra det udvalg, der er nedsat ved artikel 93, stk. 1, i forordning (EU) 2016/679 —

VEDTAGET DENNE AFGØRELSE:

Artikel 1

1. Med henblik på artikel 45 i forordning (EU) 2016/679 sikrer Republikken Korea et tilstrækkeligt beskyttelsesniveau for personoplysninger, som overføres fra Den Europæiske Union til enheder i Republikken Korea, der er omfattet af lov om beskyttelse af personoplysninger, suppleret med de yderligere garantier i bilag I og de officielle redegørelser, forsikringer og tilsagn i bilag II.

2. Denne afgørelse omfatter ikke personoplysninger, der overføres til modtagere, som tilhører en af følgende kategorier, for så vidt hele eller en del af formålet med behandlingen af personoplysningerne svarer til et af de heri anførte formål:

a) religiøse organisationer, i det omfang de behandler personoplysninger i forbindelse med deres missionsarbejde

b) politiske partier, i det omfang de behandler personoplysninger i forbindelse med udnævnelsen af kandidater

c) enheder, der er underlagt kommissionen for finansielle tjenesteydelsers tilsyn med behandlingen af personlige kreditoplysninger i medfør af lov om kreditoplysninger, i det omfang de behandler sådanne oplysninger.

Artikel 2

Når de kompetente myndigheder i medlemsstaterne med henblik på at beskytte personer i forbindelse med behandling af deres personoplysninger udøver deres beføjelser i henhold til artikel 58 i forordning (EU) 2016/679 med hensyn til videregivelse af oplysninger, der er omfattet af anvendelsesområdet i artikel 1 i denne afgørelse, underretter den berørte medlemsstat straks Kommissionen herom.

Artikel 3

1. Kommissionen overvåger løbende anvendelsen af den retlige ramme, som denne afgørelse er baseret på, herunder betingelserne for videreoverførsel, udøvelse af individuelle rettigheder og Republikken Koreas offentlige myndigheders adgang til oplysninger, der overføres på baggrund af denne afgørelse, med henblik på at vurdere, om Republikken Korea fortsat sikrer et tilstrækkeligt beskyttelsesniveau i henhold til artikel 1.

([387]) Udtalelse 32/2021 om Kommissionens udkast til gennemførelsesafgørelse i henhold til forordning (EU) 2016/679 om tilstrækkeligheden af beskyttelsesniveauet for personoplysninger i Republikken Korea, som findes på følgende link: https://edpb.europa.eu/our-work-tools/our-documents/opinion-art-70/opinion-322021-regarding-european-commission-draft_da.

2. Medlemsstaterne og Kommissionen underretter hinanden om tilfælde, hvor kommissionen for beskyttelse af personoplysninger eller andre kompetente koreanske myndigheder ikke sikrer overholdelsen af de retlige rammer, som denne afgørelse er baseret på.

3. Medlemsstaterne og Kommissionen underretter hinanden, hvis der er tegn på, at de koreanske myndigheders indgriben i den enkeltes ret til beskyttelse af sine personoplysninger går videre, end hvad der er strengt nødvendigt, eller på, at der ikke er en effektiv retsbeskyttelse mod sådanne indgreb.

4. Kommissionen foretager tre år efter datoen for meddelelse af denne afgørelse til medlemsstaterne og herefter mindst hvert fjerde år en evaluering af konklusionen i artikel l, stk. 1, på grundlag af alle tilgængelige oplysninger, herunder de oplysninger, der modtages som led i den årlige revision, som foretages sammen med de relevante koreanske myndigheder.

5. Dersom Kommissionen har oplysninger om, at der ikke længere sikres et tilstrækkeligt beskyttelsesniveau, underretter den de kompetente koreanske myndigheder herom. Den kan om nødvendigt beslutte at suspendere, ændre eller ophæve denne afgørelse eller begrænse dens anvendelsesområde i overensstemmelse med artikel 45, stk. 5, i forordning (EU) 2016/679, navnlig når der er tegn på:

a) at dataansvarlige i Korea, som har modtaget personoplysninger fra Den Europæiske Union i henhold til denne afgørelse, ikke efterlever de yderligere garantier i bilag I, eller at der er utilstrækkeligt tilsyn i denne henseende

b) at de koreanske myndigheder ikke efterlever de redegørelser, forsikringer og tilsagn, som er indeholdt i bilag II, herunder med hensyn til betingelserne og begrænsningerne for de koreanske myndigheders indsamling af og adgang til de i henhold til denne afgørelse overførte personoplysninger med henblik på strafferetlig håndhævelse eller af nationale sikkerhedshensyn.

Kommissionen kan også vedtage sådanne foranstaltninger, hvis de koreanske myndigheders manglende samarbejdsvilje forhindrer Kommissionen i at afgøre, om Republikken Korea fortsat sikrer et tilstrækkeligt beskyttelsesniveau.

Artikel 4

Denne afgørelse er rettet til medlemsstaterne.

Udfærdiget i Bruxelles, den 17. december 2021.

På Kommissionens vegne
Didier REYNDERS
Medlem af Kommissionen

BILAG I

SUPPLERENDE REGLER FOR FORTOLKNING OG ANVENDELSE AF LOV OM BESKYTTELSE AF PERSONOPLYSNINGER I FORBINDELSE MED BEHANDLING AF PERSONOPLYSNINGER, DER OVERFØRES TIL KOREA

Indholdsfortegnelse

I. **Oversigt**

Korea og Den Europæiske Union (i det følgende benævnt »EU«) har haft drøftelser om tilstrækkeligheden af beskyttelsesniveauet, og Europa-Kommissionen har i denne forbindelse fastslået, at Korea sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger i henhold til artikel 45 i den generelle forordning om databeskyttelse.

I denne forbindelse vedtog kommissionen for beskyttelse af personoplysninger denne meddelelse på grundlag af artikel 5 (statslige forpligtelser mv.) og artikel 14 (internationalt samarbejde) ([1]) i lov om beskyttelse af personoplysninger for at præcisere fortolkningen, anvendelsen og håndhævelsen af visse bestemmelser i loven, herunder om behandling af personoplysninger, der overføres til Korea på grundlag af EU's afgørelse om tilstrækkeligheden af beskyttelsesniveauet.

Da denne meddelelse har status af en administrativ regel, som det kompetente forvaltningsorgan fastlægger og bekendtgør for at præcisere standarderne for fortolkning, anvendelse og håndhævelse af lov om beskyttelse af personoplysninger i Koreas retssystem, har den juridisk bindende virkning for den persondataansvarlige i den forstand, at enhver overtrædelse af denne meddelelse kan betragtes som en overtrædelse af de relevante bestemmelser i PIPA. Hvis personlige rettigheder og interesser krænkes som følge af en overtrædelse af denne meddelelse, har de berørte personer desuden ret til at indgive en klage til kommissionen for beskyttelse af personoplysninger eller få prøvet deres sag ved domstolene.

Hvis den persondataansvarlige, der behandler de personoplysninger, som overføres til Korea i henhold til EU's afgørelse om tilstrækkeligheden af beskyttelsesniveauet, ikke træffer foranstaltninger, der er i overensstemmelse med denne meddelelse, vil det derfor blive vurderet, at der er »vægtige grunde til at antage, at der er sket en overtrædelse i forbindelse med personoplysninger, og at en undladelse af at handle sandsynligvis vil forårsage skade, der er vanskelig

([1]) I henhold til artikel 14 i lov om beskyttelse af personoplysninger har den koreanske regering beføjelse til at fastlægge politikker til forbedring af beskyttelsen af personoplysninger i det internationale miljø og til at forebygge krænkelser af registreredes rettigheder som følge af grænseoverskridende overførsel af personoplysninger.

at afhjælpe«, jf. lovens artikel 64, stk. 1 og 2. I sådanne tilfælde kan kommissionen for beskyttelse af personoplysninger eller tilknyttede centrale forvaltningsorganer pålægge den pågældende persondataansvarlige at træffe korrigerende foranstaltninger mv. i henhold til bemyndigelsen i denne bestemmelse, og afhængigt af de specifikke overtrædelser af loven kan der også pålægges en tilsvarende straf (sanktioner, administrative bøder mv.).

II. **Definitioner**

Definitionerne af anvendte udtryk:

i) Loven: lov om beskyttelse af personoplysninger (lov nr. 16930, ændret den 4. februar 2020 og gennemført den 5. august 2020)

ii) Præsidentielt dekret: gennemførelsesdekret til lov om beskyttelse af personoplysninger (præsidentielt dekret nr. 30509 af 3. marts 2020, ændrer andre love)

iii) Den registrerede: en fysisk person, der kan identificeres ved hjælp af de oplysninger, der behandles, og som oplysningerne således vedrører

iv) Den persondataansvarlige: en offentlig institution, juridisk person, organisation, fysisk person mv., der behandler personoplysninger direkte eller indirekte som led i sine aktiviteter

v) EU: EU (ved udgangen af februar 2020 var der 27 medlemslande ([2]), herunder Belgien, Tyskland, Frankrig, Italien, Luxembourg, Nederlandene, Danmark, Irland, Grækenland, Portugal, Spanien, Østrig, Finland, Sverige, Cypern, Tjekkiet, Estland, Ungarn, Letland, Litauen, Malta, Polen, Slovakiet, Slovenien, Rumænien, Bulgarien og Kroatien) samt lande, der er associeret med EU gennem EØS-aftalen (Island, Liechtenstein, Norge).

vi) Den generelle forordning om databeskyttelse: EU's generelle lovgivning om beskyttelse af personoplysninger, generel forordning om databeskyttelse (forordning (EU) 2016/679)

vii) Afgørelse om tilstrækkeligheden af beskyttelsesniveauet: I henhold til artikel 45, stk. 3, i den generelle forordning om databeskyttelse kan Europa-Kommissionen fastslå, at et tredjeland, et område eller en eller flere specifikke sektorer i et tredjeland eller en international organisation sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger.

III. **Supplerende regler**

1. **Begrænsning i ikkeformålsbestemt anvendelse og videregivelse af personoplysninger (lovens artikel 3, 15 og 18)**

<Lov om beskyttelse af personoplysninger

(Lov nr. 16930, delvis ændret den 4. februar 2020)>

Artikel 3 (principper for beskyttelse af personoplysninger) 1. Den persondataansvarlige angiver udtrykkeligt de formål, hvortil personoplysninger behandles, og indsamler personoplysninger på lovlig og rimelig vis i mindst muligt omfang for at nå disse formål.

2. Den persondataansvarlige behandler personoplysninger på en hensigtsmæssig måde, der er nødvendig til de formål, hvortil personoplysningerne behandles, og anvender dem ikke til andre formål.

Artikel 15 (indsamling og anvendelse af personoplysninger) 1. Den persondataansvarlige kan indsamle personoplysninger i følgende tilfælde og anvende dem inden for rammerne af formålet med indsamlingen:

1. Hvis der er indhentet samtykke fra en registreret.

2. Hvis der findes særlige bestemmelser i lovgivningen, eller hvis det er nødvendigt for at overholde retlige forpligtelser.

3. Hvis det er nødvendigt for, at en offentlig institution kan varetage de opgaver, som hører under dens kompetence i henhold til lovgivningen mv.

4. Hvis det er nødvendigt for at gennemføre og opfylde en kontrakt med en registreret.

([2]) Indtil overgangsperiodens udløb omfatter dette også Det Forenede Kongerige, jf. artikel 126, 127 og 132 i aftalen om Det Forenede Kongerige Storbritannien og Nordirlands udtræden af Den Europæiske Union og Det Europæiske Atomenergifællesskab (2019/C 384 I/01).

5. Hvis det skønnes at være åbenbart nødvendigt for at beskytte den registreredes eller tredjemands liv, legeme eller ejendom mod overhængende fare, hvis den registrerede eller dennes retlige repræsentant ikke er i stand til at tilkendegive sin hensigt, eller hvis forudgående samtykke ikke kan opnås på grund af ukendte adresser mv.

6. Hvis det er nødvendigt for at beskytte den persondataansvarliges berettigede interesse, hvis denne interesse går klart forud for den registreredes rettigheder. I sådanne tilfælde er behandling kun tilladt, i det omfang behandlingen i væsentlig grad vedrører den persondataansvarliges berettigede interesse og holdes inden for et rimeligt omfang.

Artikel 18 (begrænsning i ikkeformålsbestemt anvendelse og videregivelse af personoplysninger) 1. Den persondataansvarlige må ikke anvende personoplysninger uden for rammerne af det anvendelsesområde, der er fastsat i artikel 15, stk. 1, og artikel 39-3, stk. 1 og 2, eller videregive dem til tredjemand uden for rammerne af det anvendelsesområde, der er fastsat i artikel 17, stk. 1 og 3.

2. Uanset stk. 1 kan en persondataansvarlig, hvis et eller flere af følgende afsnit finder anvendelse, anvende personoplysninger eller videregive dem til tredjemand til andre formål, medmindre det er sandsynligt, at det vil krænke den registreredes eller tredjemands interesser uretmæssigt: Udbydere af informations- og kommunikationstjenester [som fastsat i artikel 2, stk. 1, nr. 3, i lov om fremme af anvendelsen af informations- og kommunikationsnetværk og databeskyttelse mv., herefter forstås det samme], der behandler personoplysninger om brugere [som fastsat i artikel 2, stk. 1, nr. 4, i lov om fremme af informations- og kommunikationsnettets anvendelse og informationsbeskyttelse mv., herefter forstås det samme], er kun er omfattet af nr. 1 og 2, og nr. 5-9, finder kun anvendelse på offentlige institutioner:

1. Hvis der er indhentet yderligere samtykke fra den registrerede.

2. Hvis der findes andre særlige bestemmelser i lovgivningen.

3. Hvis det skønnes at være åbenbart nødvendigt for at beskytte den registreredes eller tredjemands liv, legeme eller ejendom mod overhængende fare, hvis den registrerede eller dennes retlige repræsentant ikke er i stand til at tilkendegive sin hensigt, eller hvis forudgående samtykke ikke kan opnås på grund af ukendte adresser.

4. Slettet < ved lov nr. 16930 af 4. februar 2020 >

5. Hvis det er umuligt at varetage de opgaver, som hører under dens kompetence i henhold til lovgivning, medmindre den persondataansvarlige anvender personoplysninger til et andet formål end det tilsigtede eller videregiver dem til tredjemand, og kommissionen behandler spørgsmålet og træffer beslutning herom.

6. Hvis det er nødvendigt at videregive personoplysninger til en udenlandsk regering eller international organisation for at gennemføre en traktat eller en anden international konvention.

7. Hvis det er nødvendigt for efterforskningen af en forbrydelse, tiltalerejsning og retsforfølgelse.

8. Hvis det er nødvendigt for en domstol i forbindelse med en retssag.

9. Hvis det er nødvendigt med henblik på fuldbyrdelse af straf, prøveløsladelse og varetægtsfængsling.

udeladt stk. 3 ~ stk. 4

5. Hvis den persondataansvarlige videregiver personoplysninger til tredjemand til et andet formål end det tilsigtede i de situationer, som er omhandlet i stk. 2, anmoder den persondataansvarlige modtageren af personoplysningerne om at begrænse anvendelsesformålet og -metoden og andre nødvendige elementer eller om at forberede de nødvendige garantier for at garantere personoplysningernes sikkerhed. I sådanne tilfælde træffer den person, der modtager en sådan anmodning, de nødvendige foranstaltninger for at garantere personoplysningernes sikkerhed.

i) I lovens artikel 3, stk. 1 og 2, fastsættes princippet om, at den persondataansvarlige kun må indsamle det minimum af personoplysninger, der er nødvendigt for at opfylde formålet med behandlingen af personoplysningerne på lovlig vis, og ikke må anvende dem til andre formål end det tilsigtede ([3]).

ii) I henhold til dette princip er det i lovens artikel 15, stk. 1, fastsat, at en persondataansvarlig, der indsamler personoplysninger, skal anvende personoplysningerne inden for rammerne af indsamlingsformålet, og i henhold til artikel 18, stk. 1, må personoplysningerne ikke anvendes uden for rammerne af formålet med indsamlingen eller videregivelsen til tredjemand.

([3]) Da disse bestemmelser fastsætter de generelle principper, der gælder for enhver behandling af personoplysninger, herunder når en sådan behandling er specifikt reguleret ved andre love, gælder præciseringerne i dette afsnit også, hvis personoplysninger behandles på grundlag af anden lovgivning (jf. f.eks. artikel 15, stk. 1, i lov om kreditoplysninger, hvor der henvises specifikt til disse bestemmelser).

iii) Selv om personoplysninger kan anvendes til andre formål end det tilsigtede eller videregives til tredjemand under de ekstraordinære omstændigheder ([4]), der er beskrevet i lovens artikel 18, stk. 2, skal der desuden stilles krav om, at anvendelsesformålet eller -metoden begrænses, således at personoplysninger kan behandles sikkert i henhold til stk. 5, eller at der træffes de nødvendige foranstaltninger til at garantere personoplysningernes sikkerhed.

iv) Ovenstående bestemmelser finder tilsvarende anvendelse på behandling af alle personoplysninger, der modtages inden for Koreas retlige jurisdiktion fra et tredjeland, uanset den registreredes nationalitet.

v) Hvis en dataansvarlig i EU f.eks. overfører personoplysninger til en koreansk persondataansvarlig i henhold til Europa-Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet, anses den EU-dataansvarliges formål med at overføre personoplysningerne for at være den koreanske persondataansvarliges formål med at indsamle personoplysninger, og i sådanne tilfælde må den koreanske persondataansvarlige kun anvende personoplysningerne eller videregive dem til tredjemand inden for rammerne af indsamlingsformålet, undtagen under de ekstraordinære omstændigheder, der er beskrevet i lovens artikel 18, stk. 2.

2. **Begrænsning i videreoverførslen af personoplysninger (lovens artikel 17, stk. 3 og 4, og artikel 18)**

<Lov om beskyttelse af personoplysninger

(Lov nr. 16930, delvis ændret den 4. februar 2020)>

Artikel 17 (videregivelse af personoplysninger) 1. udeladt

2. Den persondataansvarlige underretter den registrerede om følgende forhold i forbindelse med indhentningen af samtykke i henhold til stk. 1, nr. 1. Det samme gælder, når følgende forhold ændres:

1. Modtageren af personoplysninger.

2. Det formål, hvortil modtageren af personoplysninger anvender sådanne oplysninger.

3. Nærmere oplysninger om de personoplysninger, der skal videregives.

4. Den periode, hvori modtageren opbevarer og anvender personoplysninger.

5. Den registreredes ret til at nægte samtykke og eventuelle ulemper som følge heraf.

3. Den persondataansvarlige underretter den registrerede om de forhold, der er omhandlet i stk. 2, og indhenter samtykke fra den registrerede med henblik på at videregive personoplysninger til en tredjemand i udlandet og må ikke indgå en aftale om grænseoverskridende overførsel af personoplysninger i strid med denne lov.

4. Den persondataansvarlige kan videregive personoplysninger uden den registreredes samtykke inden for rammer, der er rimeligt relateret til det oprindelige formål med indsamlingen, i overensstemmelse med de elementer, der er fastsat ved præsidentielt dekret, under hensyntagen til eventuelle ulemper for den registrerede, og forudsat at de nødvendige sikkerhedsforanstaltninger, f.eks. kryptering, er blevet truffet.

※ Se s. 3, 4 og 5 vedrørende artikel 18.

<Gennemførelsesdekret til lov om beskyttelse af personoplysninger

([Gennemførelsesdato: 5. februar 2021.] [Præsidentielt dekret nr. 30892 af 4. august 2020, ændrer andre love])>

Artikel 14-2 (standarder for yderligere anvendelse eller videregivelse af personoplysninger mv.)

1. Hvis en persondataansvarlig anvender eller videregiver personoplysninger (herefter »yderligere anvendelse eller videregivelse af personoplysninger«) uden den registreredes samtykke i overensstemmelse med lovens artikel 15, stk. 3, eller lovens artikel 17, stk. 4, tager den persondataansvarlige følgende forhold i betragtning:

1. Om de er rimeligt relateret til det oprindelige formål med indsamlingen af personoplysningerne.

2. Om yderligere anvendelse eller videregivelse af personoplysninger er forventelig i lyset af de omstændigheder, hvorunder personoplysningerne blev indsamlet, og behandlingspraksis.

3. Om yderligere anvendelse eller videregivelse af personoplysninger ikke krænker den registreredes interesser uretmæssigt.

4. Om de nødvendige foranstaltninger til at garantere sikkerheden, f.eks. pseudonymisering eller kryptering, er truffet.

([4]) Udbydere af informationstjenester er kun omfattet af artikel 18, stk. 2, nr. 1 og 2. Punkt 5-9 finder kun anvendelse på offentlige institutioner.

2. Den persondataansvarlige offentliggør på forhånd kriterierne for vurdering af de i stk. 1 omhandlede forhold i politikken for beskyttelse af privatlivets fred i henhold til lovens artikel 30, stk. 1, og den databeskyttelsesansvarlige i henhold til lovens artikel 31, stk. 1, kontrollerer, om den persondataansvarlige anvender eller videregiver yderligere personoplysninger i overensstemmelse med de relevante standarder.

i) Hvis den persondataansvarlige videregiver personoplysninger til en tredjemand i udlandet, skal vedkommende på forhånd underrette de registrerede om alle de forhold, der er beskrevet i lovens artikel 17, stk. 2, og indhente deres samtykke, undtagen i tilfælde, der falder ind under stk. 1 eller 2. Der må ikke indgås aftaler om grænseoverskridende videregivelse af personoplysninger i strid med denne lov.

1) Hvis personoplysninger videregives inden for rammer, der er rimeligt relateret til det oprindelige formål med indsamlingen, i henhold til lovens artikel 17, stk. 4. Anvendelsen af denne bestemmelse er imidlertid begrænset til tilfælde, hvor standarderne for yderligere anvendelse eller videregivelse af personoplysninger i artikel 14-2 i gennemførelsesdekretet er opfyldt. Desuden skal den persondataansvarlige overveje, om videregivelsen af personoplysninger kan være til ulempe for de registrerede, og om vedkommende har truffet de nødvendige foranstaltninger til at garantere sikkerheden, f.eks. kryptering.

2) Hvis personoplysninger kan videregives til tredjemand under de ekstraordinære omstændigheder, der er beskrevet i lovens artikel 18, stk. 2 (se s. 3 ~ 5). Selv under disse omstændigheder kan personoplysningerne imidlertid ikke videregives til tredjemand, hvis det er sandsynligt, at videregivelsen af sådanne personoplysninger uretmæssigt vil krænke den registreredes eller tredjemands interesser. Desuden skal leverandøren af personoplysningerne anmode modtageren af personoplysningerne om at begrænse formålet med eller metoden for anvendelse af personoplysningerne eller træffe de nødvendige foranstaltninger til at garantere sikkerheden heraf, således at personoplysningerne kan behandles sikkert.

ii) Personoplysninger, der videregives til tredjemand i udlandet, er ikke altid sikret det beskyttelsesniveau, der er garanteret i Koreas lov om beskyttelse af personoplysninger på grund af forskelle i de forskellige landes systemer til beskyttelse af personoplysninger. Sådanne sager vil derfor blive betragtet som »sager, hvor der kan være ulemper for den registrerede« som omhandlet i lovens artikel 17, stk. 4, eller »sager, hvor den registreredes eller tredjemands interesser krænkes uretmæssigt«, som omhandlet i lovens artikel 18, stk. 2, og artikel 14-2 i gennemførelsesdekretet til samme lov ([5]). For at opfylde kravene i disse bestemmelser skal den persondataansvarlige og tredjemand derfor udtrykkeligt garantere et beskyttelsesniveau svarende til lovens, herunder at den registrerede kan udøve sine rettigheder, i juridisk bindende dokumenter såsom kontrakter, selv efter overførslen af personoplysningerne til udlandet.

3. **Underretning om oplysningerne, hvis personoplysningerne ikke er indsamlet hos den registrerede (lovens artikel 20)**

<Lov om beskyttelse af personoplysninger

(Lov nr. 16930, delvis ændret den 4. februar 2020)>

Artikel 20 (underretning om kilder mv. til personoplysninger indsamlet fra tredjemand) 1. En persondataansvarlig, der behandler personoplysninger indsamlet fra tredjemand, underretter straks den registrerede om følgende forhold på dennes anmodning:

1. Kilden til indsamlede personoplysninger.

2. Formålet med behandlingen af personoplysninger.

3. Den registreredes ret til at kræve, at behandlingen af personoplysninger suspenderes, jf. artikel 37.

2. Uanset stk. 1 underretter en persondataansvarlig, der opfylder kriterierne fastsat ved præsidentielt dekret, under hensyntagen til typen og mængden af behandlede personoplysninger, antallet af ansatte, salgsmængde mv., og indsamler personoplysninger fra tredjemand og behandler disse i henhold til artikel 17, stk. 1, nr. 1, den registrerede om de elementer, der er omhandlet i stk. 1. Dette gælder dog ikke, hvis de oplysninger, der indsamles af den persondataansvarlige, ikke indeholder personoplysninger, f.eks. kontaktoplysninger, der kan anvendes til at underrette den registrerede.

([5]) I henhold til artikel 18, stk. 2, nr. 2, i PIPA gælder dette også, når personoplysninger videregives til tredjemand i udlandet på grundlag af bestemmelser i andre love (f.eks. lov om kreditoplysninger).

3. Nødvendige elementer vedrørende frist, metode og procedure for underretning af den registrerede i henhold til hovedbestemmelsen i stk. 2 fastsættes ved præsidentielt dekret.

4. Stk. 1 og hovedbestemmelsen i stk. 2 finder ikke anvendelse i følgende tilfælde: Dette gælder dog ikke, hvis underretningen går klart forud for de registreredes rettigheder i henhold til denne lov:

1. Hvis personoplysninger, der er genstand for en anmodning om underretning, indgår i persondatafilerne omhandlet i artikel 32, stk. 2.

2. Hvis en sådan underretning sandsynligvis vil skade en anden persons liv eller legeme eller uretmæssigt skader en anden persons ejendom og andre interesser.

i) Hvis den persondataansvarlige modtager personoplysninger overført fra EU på grundlag af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet ([6]), skal vedkommende uden unødig forsinkelse og under alle omstændigheder senest en måned efter overførslen give den registrerede følgende oplysninger i nr. 1)-5).

1) Navn og kontaktoplysninger på de personer, der overfører og modtager personoplysningerne.

2) De elementer eller kategorier af personoplysninger, der overføres.

3) Formålet med at indsamle og anvende personoplysningerne (som fastsat af dataeksportøren i henhold til punkt 1 i denne meddelelse).

4) Opbevaringsperioden for personoplysninger.

5) Oplysninger om den registreredes rettigheder i forbindelse med behandlingen af personoplysninger, måden og proceduren for udøvelse af rettighederne og eventuelle ulemper som følge af udøvelsen heraf.

ii) Hvis den persondataansvarlige videregiver personoplysningerne i nr. i) til en tredjemand i Republikken Korea eller i udlandet, skal vedkommende også give den registrerede oplysningerne i nr. 1)-5), inden personoplysningerne videregives.

1) Navn og kontaktoplysninger på de personer, der videregiver og modtager personoplysningerne.

2) De elementer eller kategorier af personoplysninger, der videregives.

3) Det land, hvortil personoplysningerne skal videregives, den forventede dato og metode for videregivelsen (begrænset til tilfælde, hvor personoplysninger skal videregives til en tredjemand i udlandet).

4) Videregiveren af personoplysningernes formål og retsgrundlaget for videregivelse af personoplysningerne.

5) Oplysninger om den registreredes rettigheder i forbindelse med behandlingen af personoplysninger, måden og proceduren for udøvelse af rettighederne og eventuelle ulemper som følge af udøvelsen heraf.

iii) Den persondataansvarlige må ikke anvende nr. i) eller ii) i følgende tilfælde (nr. 1)-4)).

1) Hvis de personoplysninger, der skal meddeles, indgår i en af følgende persondatafiler som omhandlet i lovens artikel 32, stk. 2, i det omfang de interesser, der beskyttes ved denne bestemmelse, går klart forud for den registreredes rettigheder, og kun så længe underretningen vil true forfølgelsen af de berørte interesser, f.eks. ved at bringe igangværende strafferetlige efterforskninger i fare eller true den nationale sikkerhed.

2) Hvis og så længe underretningen sandsynligvis vil skade en anden persons liv eller legeme eller uretmæssigt krænke en anden persons ejendomsinteresser, hvis disse rettigheder eller interesser går klart forud for den registreredes rettigheder.

3) Hvis den registrerede allerede er i besiddelse af de oplysninger, som den persondataansvarlige skal give i henhold til nr. i) eller ii).

4) Hvis den persondataansvarlige ikke har nogen kontaktoplysninger på den registrerede, eller hvis det indebærer en uforholdsmæssig stor indsats at kontakte den registrerede, herunder i forbindelse med behandling på de betingelser, der er fastsat i afdeling 3 i PIPA. Ved afgørelsen af, om det er muligt at kontakte den registrerede, eller om dette indebærer en uforholdsmæssig stor indsats, bør der tages hensyn til muligheden for at samarbejde med dataeksportøren i EU.

([6]) Forpligtelserne i henhold til nr. i), ii) og iii) gælder ligeledes, når den dataansvarlige, der modtager personoplysninger fra EU på grundlag af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet, behandler sådanne oplysninger på grundlag af andre love, f.eks. lov om kreditoplysninger.

4. **Anvendelsesområde for den særlige undtagelse for behandling af pseudonymiserede oplysninger (lovens artikel 28-2, 28-3, 28-4, 28-5, 28-6 og 28-7, artikel 3 og artikel 58-2)**

<Lov om beskyttelse af personoplysninger

(Lov nr. 16930, delvis ændret den 4. februar 2020)>

Kapitel III Behandling af personoplysninger

AFDELING 3 Særlige sager vedrørende pseudonyme oplysninger

Artikel 28-2 (behandling af pseudonyme oplysninger) 1. Den persondataansvarlige kan behandle pseudonymiserede oplysninger uden de registreredes samtykke til statistiske formål, videnskabelige forskningsformål og arkivformål i samfundets interesse mv.

2. Den persondataansvarlige må ikke medtage oplysninger, der kan anvendes til at identificere en bestemt person, ved videregivelsen af pseudonymiserede oplysninger til tredjemand i henhold til stk. 1.

Artikel 28-3 (begrænsning af samkøring af pseudonyme data) 1. Uanset artikel 28-2 skal samkøringen af pseudonymiserede oplysninger, der behandles af forskellige persondataansvarlige til statistiske formål og med henblik på videnskabelig forskning og opbevaring af fortegnelser i samfundets interesse mv., foretages af en specialiseret institution, der er udpeget af beskyttelseskommissionen eller lederen af det tilknyttede centrale forvaltningsorgan.

2. En persondataansvarlig, der agter at eksportere de samkørte oplysninger fra den organisation, der samkørte oplysningerne, indhenter lederen af den specialiserede institutions godkendelse efter pseudonymisering af oplysningerne eller anden behandling som omhandlet i artikel 58-2.

3. Nødvendige elementer, herunder samkøringsprocedurer og -metoder i henhold til stk. 1, standarder og procedurer for udpegning eller tilbagekaldelse af udpegningen af ledelsen af og tilsynet med en specialiseret institution og standarder og procedurer for eksport og godkendelse i henhold til stk. 2 fastsættes ved præsidentielt dekret.

Artikel 28-4 (forpligtelse til at træffe sikkerhedsforanstaltninger i forbindelse med pseudonyme oplysninger) 1. Ved behandling af pseudonymiserede oplysninger træffer den persondataansvarlige de tekniske, organisatoriske og fysiske foranstaltninger, herunder separat opbevaring og forvaltning af yderligere oplysninger, der er nødvendige for at genoprette oplysningerne til deres oprindelige tilstand), alt efter hvad der er nødvendigt for at garantere sikkerheden i henhold til præsidentielt dekret, således at personoplysningerne ikke går tabt, stjæles, videregives, forfalskes, ændres eller beskadiges.

2. En persondataansvarlig, der agter at behandle pseudonymiserede oplysninger, udarbejder og fører fortegnelser over elementer fastsat ved præsidentielt dekret, herunder om formålet med behandlingen af pseudonymiserede oplysninger og om tredjepartsmodtageren i forbindelse med videregivelsen af pseudonymiserede oplysninger, med henblik på at forvalte behandlingen af pseudonymiserede oplysninger.

Artikel 28-5 (forbudte handlinger i forbindelse med behandlingen af pseudonymiserede oplysninger) 1. Det er forbudt at behandle pseudonymiserede oplysninger med det formål at identificere en bestemt person.

2. Hvis der frembringes oplysninger, som identificerer en bestemt person, i forbindelse med behandlingen af pseudonymiserede oplysninger, indstiller den persondataansvarlige straks behandlingen af oplysningerne og udtrækker og tilintetgør oplysningerne.

Artikel 28-6 (pålæggelse af administrative tillægsgebyrer for behandling af pseudonymiserede oplysninger) 1. Kommissionen kan pålægge dataansvarlige, der har behandlet oplysninger med det formål at identificere en bestemt person i strid med artikel 28-5, stk. 1, en bøde på højst trehundrededele af det samlede salg: Hvis der ikke er noget salg eller det er vanskeligt at beregne salgsindtægterne, kan den dataansvarlige pålægges en bøde på højst 400 mio. WON eller trehundrededele af kapitalbeløbet, alt efter hvad der er størst.

2. Artikel 34-2, stk. 3-5, finder tilsvarende anvendelse på elementer, der er nødvendige for at pålægge og opkræve administrative tillægsgebyrer.

Artikel 28-7 (anvendelsesområde) @ artikel 20, 21 og 27, artikel 34, stk. 1, artikel 35-37 og 39-3, 39-4 og 39-6 til 39-8 finder ikke anvendelse på pseudonymiserede oplysninger.

Kapitel I Almindelige bestemmelser

Artikel 3 (principper for beskyttelse af personoplysninger) 1. Den persondataansvarlige angiver udtrykkeligt de formål, hvortil personoplysninger behandles, og indsamler personoplysninger på lovlig og rimelig vis i mindst muligt omfang for at nå disse formål.

2. Den persondataansvarlige behandler personoplysninger på en hensigtsmæssig måde, der er nødvendig til de formål, hvortil personoplysningerne behandles, og anvender dem ikke til andre formål.

3. Den persondataansvarlige sikrer, at personoplysninger er korrekte, fuldstændige og ajourførte, i det omfang det er nødvendigt i forhold til de formål, hvortil personoplysningerne behandles.

4. Den persondataansvarlige behandler personoplysninger sikkert i overensstemmelse med behandlingsmetoder, typer mv. af personoplysninger under hensyntagen til risikoen for krænkelse af den registreredes rettigheder og alvoren af de pågældende risici.

5. Den persondataansvarlige offentliggør sin politik for beskyttelse af privatlivets fred og andre spørgsmål vedrørende behandling af personoplysninger og garanterer den registreredes rettigheder såsom retten til indsigt i egne personoplysninger.

6. Den persondataansvarlige behandler personoplysninger på en måde, der minimerer risikoen for at krænke den registreredes ret til privatlivets fred.

7. Hvis det stadig er muligt at opfylde formålet med indsamlingen af personoplysninger ved at behandle anonymiserede eller pseudonymiserede personoplysninger, bestræber den persondataansvarlige sig på at behandle personoplysninger gennem anonymisering, hvis anonymisering er mulig, eller gennem pseudonymisering, hvis det er umuligt at opfylde formålet med indsamlingen af personoplysninger gennem anonymisering.

8. Den persondataansvarlige bestræber sig på at vinde de registreredes tillid ved at overholde og udføre de opgaver og ansvarsområder, der er fastsat i denne lov og andre relaterede love.

Kapitel IX Supplerende bestemmelser

Artikel 58-2 (undtagelse fra anvendelse) Denne lov finder ikke anvendelse på oplysninger, der ikke længere identificerer en bestemt person, når de samkøres med andre oplysninger, under rimelig hensyntagen til tid, omkostninger, teknologi mv. <Denne artikel er indsat for nylig ved lov nr. 16930 af 4. februar 2020 >

i) Kapitel III, afdeling 3 om særlige tilfælde vedrørende pseudonyme oplysninger (artikel 28-2 til 28-7) giver mulighed for behandling af pseudonymiserede oplysninger uden den registreredes samtykke til statistiske formål og med henblik på videnskabelig forskning og opbevaring af offentlige fortegnelser mv. (artikel 28-2), men i sådanne tilfælde skal der indføres de fornødne garantier og forbud for at beskytte de registreredes rettigheder (artikel 28-4 og 28-5), lovovertrædere kan pålægges tillægssanktioner (artikel 28-6), og visse garantier i PIPA finder ikke anvendelse (artikel 28-7).

ii) Disse bestemmelser finder ikke anvendelse i tilfælde, hvor pseudonymiserede oplysninger behandles til andre formål end udarbejdelse af statistikker, videnskabelig forskning, opbevaring af offentlige fortegnelser mv. Hvis en EU-borgers personoplysninger, der er overført til Korea i henhold til Europa-Kommissionens afgørelse om tilstrækkeligheden af beskyttelsesniveauet, f.eks. pseudonymiseres til andre formål end udarbejdelse af statistikker, videnskabelig forskning, opbevaring af offentlige fortegnelser mv., finder de særlige bestemmelser i kapitel III, afdeling 3, ikke anvendelse ([7]).

iii) Hvis den persondataansvarlige behandler pseudonymiserede oplysninger med henblik på udarbejdelse af statistikker, videnskabelig forskning, opbevaring af offentlige fortegnelser mv., og de pseudonymiserede oplysninger ikke er blevet tilintetgjort, når det specifikke formål med behandlingen er opfyldt, i overensstemmelse med forfatningens artikel 37 og lovens artikel 3 (principper for beskyttelse af personoplysninger), anonymiserer den dataansvarlige oplysningerne for at sikre, at de ikke længere identificerer en bestemt person alene eller samkørt med andre oplysninger, under rimelig hensyntagen til tid, omkostninger, teknologi mv., i overensstemmelse med artikel 58-2 i PIPA.

5. **Korrigerende foranstaltninger mv. (lovens artikel 64, stk. 1, 2 og 4)**

<Lov om beskyttelse af personoplysninger

(Lov nr. 16930, delvis ændret den 4. februar 2020)>

Artikel 64 (korrigerende foranstaltninger) 1. Hvis beskyttelseskommissionen finder, at der er vægtige grunde til at antage, at der er sket en overtrædelse i forbindelse med personoplysninger, og at en undladelse af at handle sandsynligvis vil forårsage skade, der er vanskelig at afhjælpe, kan kommissionen pålægge lovovertræderen (dog ikke centrale forvaltningsorganer, lokale myndigheder, nationalforsamlingen, retten, forfatningsdomstolen og den nationale valgkommission) at træffe følgende foranstaltninger:

1. Standse overtrædelser i forbindelse med personoplysninger.

2. Midlertidigt suspendere behandlingen af personoplysninger.

([7]) Tilsvarende finder undtagelsen i artikel 40-3 i lov om kreditoplysninger kun anvendelse på behandling af pseudonymiserede kreditoplysninger med henblik på udarbejdelse af statistikker, videnskabelig forskning og opbevaring af offentlige fortegnelser.

3. Andre nødvendige foranstaltninger til at beskytte personoplysninger og forebygge overtrædelser i forbindelse med personoplysninger.

2. Hvis lederen af et tilknyttet centralt forvaltningsorgan finder, at der er vægtige grunde til at antage, at der er sket en overtrædelse i forbindelse med personoplysninger, og at en undladelse af at handle sandsynligvis vil forårsage skade, der er vanskelig at afhjælpe, kan lederen pålægge en persondataansvarlig at træffe en af de foranstaltninger, der er omhandlet i stk. 1, i henhold til lovgivningen i det tilknyttede centrale forvaltningsorgans jurisdiktion.

4. Hvis et centralt forvaltningsorgan, en lokal myndighed, nationalforsamlingen, retten, forfatningsdomstolen eller den nationale valgkommission overtræder denne lov, kan beskyttelseskommissionen henstille til lederen af det relevante organ at træffe de foranstaltninger, der er omhandlet i stk. 1. I sådanne tilfælde følger organet henstillingen, når den er modtaget, medmindre der foreligger ekstraordinære omstændigheder.

i) For det første fortolker retspraksis ([8]) ([9]) »skade, der er vanskelig at afhjælpe« som en skade, der kan krænke den enkeltes personlige rettigheder eller ret til privatlivets fred.

ii) Ved »vægtige grunde til at antage, at der er sket en overtrædelse i forbindelse med personoplysninger, og at en undladelse af at handle sandsynligvis vil forårsage skade«, jf. artikel 64, stk. 1 og 2, forstås således tilfælde, hvor en overtrædelse af loven anses for at kunne krænke den enkeltes rettigheder og friheder med hensyn til beskyttelse af deres personoplysninger. Dette er tilfældet, hver gang en af de principper, rettigheder og forpligtelser, der er indeholdt i lov om beskyttelse af personoplysninger, krænkes ([10]).

iii) I henhold til artikel 64, stk. 4, i lov om beskyttelse af personoplysninger er en foranstaltning i forbindelse med »overtrædelse af denne lov« en foranstaltning mod en overtrædelse af PIPA.

Et centralt forvaltningsorgan mv. som en offentlig myndighed, der er forpligtet til at overholde retsstatsprincippet, må ikke overtræde lovgivningen og er forpligtet til at træffe en korrigerende foranstaltning, herunder til straks at bringe handlingen til ophør, og yde erstatning i de ekstraordinære tilfælde, hvor der ikke desto mindre blev begået en ulovlig handling.

Selv uden beskyttelseskommissionens indgreb i henhold til artikel 64, stk. 4, i PIPA skal et centralt forvaltningsorgan mv. således træffe en korrigerende foranstaltning mod overtrædelser, hvis det bliver bekendt med en overtrædelse af loven.

Hvis beskyttelseskommissionen har henstillet, at der træffes en korrigerende foranstaltning, vil det navnlig normalt være objektivt klart for det centrale forvaltningsorgan, at det har overtrådt loven. For at begrunde, hvorfor det ikke mener, at en henstilling fra beskyttelseskommissionen bør følges, skal et centralt forvaltningsorgan mv. fremlægge klare grunde, der kan bevise, at det ikke har overtrådt loven. Henstillingen skal følges, medmindre beskyttelseskommissionen fastslår, at dette rent faktisk ikke er tilfældet.

I betragtning heraf skal de »ekstraordinære omstændigheder« i artikel 64, stk. 4, i lov om beskyttelse af personoplysninger være strengt begrænset til ekstraordinære omstændigheder, hvor centrale forvaltningsorganer mv. kan fremlægge klare grunde, der beviser, at »denne lov faktisk ikke er blevet overtrådt«, såsom »tilfælde, hvor der foreligger ekstraordinære (faktiske eller retlige) omstændigheder«, som beskyttelseskommissionen ikke havde kendskab til, da den oprindeligt fremsatte sin henstilling, og beskyttelseskommissionen fastslår, at der rent faktisk ikke er sket en overtrædelse.

6. **Anvendelse af PIPA på behandling af personoplysninger til nationale sikkerhedsformål, herunder efterforskning af overtrædelser og håndhævelse i henhold til PIPA (artikel 7-8, artikel 7-9, artikel 58, artikel 3, artikel 4 og artikel 62 i PIPA)**

<Lov om beskyttelse af personoplysninger

(Lov nr. 16930, delvis ændret den 4. februar 2020)>

Artikel 7-8 (beskyttelseskommissionens arbejde) 1. Beskyttelseskommissionen varetager følgende opgaver: […]

3. Spørgsmål vedrørende undersøgelse af krænkelser af registreredes rettigheder og de deraf følgende dispositioner

4. Behandling af klager eller afhjælpende procedurer i forbindelse med behandling af personoplysninger og mægling i tvister om personoplysninger

[…]

([8]) (Højesterets dom 97Da10215,10222 af 1999. januar 26) Hvis den tiltaltes strafbare handlinger afsløres via medierne, vil det sandsynligvis forårsage uoprettelig mental og fysisk skade, ikke blot på ofret, dvs. sagsøgeren, men også på personer omkring vedkommende, herunder familier.

([9]) (Seoul High Courts dom 2006NA92006 af 2008. januar 16) Hvis der offentliggøres en ærekrænkende artikel, vil det sandsynligvis forårsage alvorlig uoprettelig skade på den involverede person.

([10]) De samme principper som dem, der er fastsat i nr. ii), finder anvendelse på artikel 45-4 i lov om kreditoplysninger.

Artikel 7-9 (spørgsmål, som beskyttelseskommissionen behandler og træffer beslutning om) 1. Beskyttelseskommissionen behandler og træffer beslutning om følgende spørgsmål: […]

5. Spørgsmål vedrørende fortolkning og anvendelse af lovgivning om beskyttelse af personoplysninger

[…]

Artikel 58 (delvis udelukkelse fra anvendelse) 1. Kapitel III-VII finder ikke anvendelse på følgende personoplysninger:

1. Personoplysninger, der indsamles i henhold til statistikloven med henblik på behandling i offentlige institutioner.
2. Personoplysninger, der indsamles eller udbedes med henblik på analyse af oplysninger vedrørende den nationale sikkerhed.
3. Personoplysninger, der behandles midlertidigt, når det er bydende nødvendigt af hensyn til den offentlige sikkerhed, folkesundheden mv.
4. Personoplysninger, der indsamles eller anvendes af pressen til egne rapporteringsformål og i forbindelse med religiøse organisationers missionsarbejde og politiske partiers udnævnelse af kandidater.

[undladt stk. 2 og 3]

4. I forbindelse med behandling af personoplysninger i henhold til stk. 1 behandler den persondataansvarlige personoplysningerne i mindst muligt omfang og ikke længere end nødvendigt for at nå det tilsigtede formål og træffer ligeledes de nødvendige foranstaltninger såsom tekniske, ledelsesmæssige og fysiske garantier, individuel klagebehandling og andre nødvendige foranstaltninger til sikker forvaltning og korrekt behandling af sådanne personoplysninger.

Artikel 3 (principper for beskyttelse af personoplysninger) 1. Den persondataansvarlige angiver udtrykkeligt de formål, hvortil personoplysninger behandles, og indsamler personoplysninger på lovlig og rimelig vis i mindst muligt omfang for at nå disse formål.

2. Den persondataansvarlige behandler personoplysninger på en hensigtsmæssig måde, der er nødvendig til de formål, hvortil personoplysningerne behandles, og anvender dem ikke til andre formål.

3. Den persondataansvarlige sikrer, at personoplysninger er korrekte, fuldstændige og ajourførte, i det omfang det er nødvendigt i forhold til de formål, hvortil personoplysningerne behandles.

4. Den persondataansvarlige behandler personoplysninger sikkert i overensstemmelse med behandlingsmetoder, typer mv. af personoplysninger under hensyntagen til risikoen for krænkelse af den registreredes rettigheder og alvoren af de pågældende risici.

5. Den persondataansvarlige offentliggør sin politik for beskyttelse af privatlivets fred og andre spørgsmål vedrørende behandling af personoplysninger og garanterer den registreredes rettigheder såsom retten til indsigt i egne personoplysninger.

6. Den persondataansvarlige behandler personoplysninger på en måde, der minimerer risikoen for at krænke den registreredes ret til privatlivets fred.

7. Hvis det stadig er muligt at opfylde formålet med indsamlingen af personoplysninger ved at behandle anonymiserede eller pseudonymiserede personoplysninger, bestræber den persondataansvarlige sig på at behandle personoplysninger gennem anonymisering, hvis det er muligt, eller gennem pseudonymisering, hvis det er umuligt at opfylde formålet med indsamlingen af personoplysninger gennem anonymisering.

8. Den persondataansvarlige bestræber sig på at vinde de registreredes tillid ved at overholde og udføre de opgaver og ansvarsområder, der er fastsat i denne lov og andre relaterede love.

Artikel 4 (registreredes rettigheder) Den registrerede har følgende rettigheder i forbindelse med behandlingen af sine personoplysninger:

1. Retten til at blive informeret om behandlingen af sådanne personoplysninger.
2. Retten til at afgøre, om der skal gives samtykke til behandling af sådanne personoplysninger, og omfanget af samtykket.
3. Retten til at få bekræftet, om personoplysninger behandles, og til at anmode om adgang (herunder udlevering af kopier, herefter forstås det samme) til sådanne personoplysninger.
4. Retten til at suspendere behandlingen af og anmode om berigtigelse, sletning og tilintetgørelse af sådanne personoplysninger.
5. Retten til passende erstatning for enhver skade, der opstår som følge af behandlingen af sådanne personoplysninger, gennem en hurtig og retfærdig procedure.

Artikel 62 (indberetning af overtrædelser) 1. Enhver, hvis rettigheder eller interesser er blevet krænket i forbindelse med den persondataansvarliges behandling af vedkommendes personoplysninger, kan indberette en sådan overtrædelse til beskyttelseskommissionen.

2. Beskyttelseskommissionen kan udpege en specialiseret institution, der skal modtage og behandle indberetninger om krænkelser effektivt i henhold til stk. 1 som fastsat ved præsidentielt dekret. I sådanne tilfælde opretter og driver en sådan specialiseret institution et callcenter for krænkelse af retten til beskyttelse af personoplysninger (»callcentret for privatlivsbeskyttelse«).

3. Callcentret for privatlivsbeskyttelse varetager følgende opgaver:

1. Modtager indberetninger om krænkelser og yder rådgivning om behandlingen af personoplysninger.

2. Undersøger og bekræfter hændelser og indhenter udtalelser fra involverede parter.

3. Opgaver i tilknytning til nr. 1 og 2.

4. Beskyttelseskommissionen kan om nødvendigt udsende en offentligt ansat til den specialiserede institution, der er udpeget i henhold til stk. 2 i medfør af artikel 32-4 i lov om offentligt ansatte, for at undersøge og bekræfte hændelserne effektivt i henhold til stk. 3, nr. 2.

i) Indsamlingen af personoplysninger til nationale sikkerhedsformål er reguleret ved specifik lovgivning, der bemyndiger de kompetente myndigheder (f.eks. den nationale efterretningstjeneste) til at aflytte kommunikation eller anmode om videregivelse på visse betingelser og med visse garantier (herefter »national sikkerhedslovgivning«). Denne nationale sikkerhedslovgivning omfatter f.eks. lov om beskyttelse af privatlivets fred i forbindelse med kommunikation, lov om bekæmpelse af terrorisme og beskyttelse af borgerne og den offentlige sikkerhed eller telekommunikationsloven. Desuden skal indsamlingen og viderebehandlingen af personoplysninger opfylde kravene i PIPA. I denne forbindelse fastsættes det i artikel 58, stk. 1, nr. 2, i PIPA, at kapitel III-VII ikke finder anvendelse på personoplysninger, der indsamles eller udbedes med henblik på analyse af oplysninger vedrørende den nationale sikkerhed. Denne delvise undtagelse gælder derfor for behandling af personoplysninger til nationale sikkerhedsformål.

Samtidig finder kapitel I (almindelige bestemmelser), kapitel II (fastlæggelse af politikker for beskyttelse af personoplysninger mv.), kapitel VIII (kollektive søgsmål vedrørende dataovertrædelser), kapitel IX (supplerende bestemmelser) og kapitel X (sanktionsbestemmelser) anvendelse på behandlingen af sådanne personoplysninger. Dette omfatter de generelle databeskyttelsesprincipper, der er fastsat i artikel 3 (principper for beskyttelse af personoplysninger) og de individuelle rettigheder, der er sikret ved artikel 4 i PIPA (registreredes rettigheder).

Desuden fastsættes det i artikel 58, stk. 4, i PIPA, at sådanne oplysninger skal behandles i mindst muligt omfang for at nå det tilsigtede formål og ikke længere end nødvendigt. Den persondataansvarlige pålægges ligeledes at træffe de nødvendige foranstaltninger til at garantere en sikker dataforvaltning og korrekt behandling såsom tekniske, ledelsesmæssige og fysiske garantier samt foranstaltninger til korrekt behandling af individuelle klager.

Endelig finder bestemmelserne om PIPC's opgaver og beføjelser (herunder artikel 60-65 i PIPA om behandling af klager og fremsættelse af henstillinger og iværksættelse af korrigerende foranstaltninger) samt bestemmelserne om administrative og strafferetlige sanktioner (artikel 70 ff. i PIPA) anvendelse. I henhold til artikel 7-8, stk. 1, nr. 3 og 4, og artikel 7-9, stk. 1, nr. 5, i PIPA omfatter disse undersøgelsesbeføjelser og beføjelser til at fastsætte korrigerende foranstaltninger, herunder når de udøves i forbindelse med behandling af klager, også mulige overtrædelser af reglerne i specifikke love, der fastsætter begrænsninger og garantier for indsamling af personoplysninger, såsom den nationale sikkerhedslovgivning. I betragtning af kravene i artikel 3, stk. 1, i PIPA vedrørende lovlig og rimelig indsamling af personoplysninger udgør en sådan overtrædelse ligeledes en overtrædelse af »denne lov«, jf. artikel 63 og 64, der giver PIPC mulighed for at foretage en undersøgelse og træffe korrigerende foranstaltninger ([11]). PIPC's udøvelse af disse beføjelser supplerer, men erstatter ikke den nationale menneskerettighedskommissions beføjelser i medfør af lov om menneskerettighedskommissionen.

Anvendelsen af de grundlæggende principper, rettigheder og forpligtelser i PIPA i forbindelse med behandlingen af personoplysninger til nationale sikkerhedsformål afspejler de garantier, der er nedfældet i forfatningen, for beskyttelse af den enkeltes ret til at kontrollere sine egne personoplysninger. Som anerkendt af forfatningsdomstolen omfatter dette en persons ret ([12]) til »selv at afgøre, hvornår, til hvem eller af hvem, og i hvilket omfang vedkommendes oplysninger vil blive videregivet eller anvendt. Det er en grundlæggende ret ([13]) […], der skal at beskytte den personlige beslutningsfrihed mod risikoen forbundet med udvidelsen af statens funktioner og informations- og kommunikationsteknologien«. Enhver begrænsning af denne ret, f.eks. når det er nødvendigt for at beskytte statens sikkerhed, kræver en afvejning af den enkeltes rettigheder og interesser i forhold til den relevante offentlige interesse og må ikke berøre rettighedens væsentligste indhold (forfatningens artikel 37, stk. 2).

([11]) For så vidt angår korrigerende foranstaltninger i henhold til artikel 64, se også afsnit 5 ovenfor.
([12]) Forfatningsdomstolens dom 99HunMa513, 2004HunMa190 af 26. maj 2005.
([13]) Forfatningsdomstolens dom 2003HunMa282 af 21. juli 2005.

Ved behandling af personoplysninger til nationale sikkerhedsformål skal den dataansvarlige (f.eks. NIS) derfor bl.a.:

1. Udtrykkeligt angive de formål, hvortil personoplysninger behandles, og indsamle personoplysninger på lovlig og rimelig vis i mindst muligt omfang for at nå disse formål (artikel 3, stk. 1, i PIPA). Den dataansvarlige indsamler og viderebehandler navnlig kun personoplysninger med henblik på at varetage opgaver i henhold til de relevante love såsom lov om den nationale efterretningstjeneste.

2. Behandle personoplysninger i mindst muligt omfang og ikke længere end nødvendigt for at nå det tilsigtede formål (artikel 58, stk. 4, i PIPA). Når formålet med behandlingen er nået, tilintetgør den dataansvarlige uigenkaldeligt personoplysningerne, medmindre yderligere opbevaring er udtrykkeligt fastsat ved lov, i hvilket tilfælde de relevante personoplysninger opbevares og forvaltes adskilt fra andre personoplysninger, og de må ikke anvendes til andre formål end det, der er angivet i loven, og tilintetgøres ved opbevaringsperiodens udløb.

3. Behandle personoplysninger på en hensigtsmæssig måde, der er nødvendig til de formål, hvortil personoplysningerne behandles, og ikke anvende dem til andre formål (artikel 3, stk. 2, i PIPA).

4. Sikre, at personoplysninger er korrekte, fuldstændige og ajourførte, i det omfang det er nødvendigt i forhold til de formål, hvortil personoplysningerne behandles (artikel 3, stk. 3, i PIPA).

5. Behandle personoplysninger sikkert i overensstemmelse med behandlingsmetoder, typer mv. af personoplysninger under hensyntagen til risikoen for krænkelser af den registreredes rettigheder og alvoren af de pågældende risici (artikel 3, stk. 4, i PIPA).

6. Offentliggøre sin politik for beskyttelse af privatlivets fred og andre spørgsmål vedrørende behandling af personoplysninger (artikel 3, stk. 5, i PIPA).

7. Behandle personoplysninger på en måde, der minimerer risikoen for at krænke den registreredes ret til privatlivets fred (artikel 3, stk. 6, i PIPA).

ii) I overensstemmelse med artikel 58, stk. 4, i PIPA træffer den dataansvarlige (f.eks. myndigheder med ansvar for national sikkerhed såsom NIS) de nødvendige foranstaltninger såsom indførelse af tekniske, ledelsesmæssige og fysiske sikkerhedsforanstaltninger for at sikre overholdelse af disse principper og korrekt behandling af personoplysninger. Dette kan f.eks. omfatte specifikke foranstaltninger til at garantere personoplysningers sikkerhed såsom begrænsninger i adgangen til personoplysninger, adgangskontrol, logfiler, målrettet uddannelse af medarbejderne i håndtering af personoplysninger mv.

I medfør af artikel 3, stk. 5, og artikel 4 i PIPA har registrerede desuden bl.a. følgende rettigheder med hensyn til personoplysninger, der behandles til nationale sikkerhedsformål:

1. Retten til at få en bekræftelse på, om vedkommendes personoplysninger behandles, samt oplysninger om behandlingen og adgang til disse oplysninger, herunder udlevering af kopier (artikel 4, stk. 1 og 3, i PIPA).

2. Retten til at få suspenderet behandlingen og til berigtigelse, sletning og tilintetgørelse af personoplysninger (artikel 4, stk. 4, i PIPA).

iii) Den registrerede kan indgive en anmodning i forbindelse med udøvelsen af disse rettigheder direkte til den dataansvarlige eller indirekte via beskyttelseskommissionen og kan bemyndige sin repræsentant hertil. Hvis den registrerede indgiver en anmodning, indrømmer den dataansvarlige straks denne ret. Den dataansvarlige kan udsætte, begrænse eller nægte udøvelsen af rettigheden, hvis det er udtrykkeligt fastsat eller uundgåeligt for at overholde andre love, i det omfang og så længe det er nødvendigt og forholdsmæssigt for at beskytte et vigtigt mål af samfundsmæssig interesse (f.eks. i det omfang og så længe indrømmelsen af rettigheden vil bringe en igangværende efterforskning i fare eller true den nationale sikkerhed), eller hvis indrømmelsen af rettigheden kan skade tredjemands liv eller legeme eller er en uberettiget krænkelse af tredjemands ejendom og andre interesser. Hvis anmodningen afslås eller begrænses, underretter den dataansvarlige straks den registrerede om årsagerne hertil. Den dataansvarlige udarbejder den metode og procedure, der gør det muligt for registrerede at indgive anmodninger, og offentliggør dem, således at de registrerede kan få kendskab hertil.

I overensstemmelse med artikel 58, stk. 4, i PIPA (krav om at sikre en korrekt behandling af individuelle klager) og artikel 4, stk. 5, i PIPA (retten til passende erstatning for enhver skade, der opstår som følge af behandlingen af personoplysninger, gennem en hurtig og retfærdig procedure) har registrerede desuden ret til at få prøvet deres sag. Dette omfatter retten til at indberette en påstået overtrædelse til centret for indberetning af overtrædelser i forbindelse med personoplysninger (i overensstemmelse med artikel 62, stk. 3, i PIPA), til at indgive en klage til PIPC i henhold til artikel 62 i PIPA om enhver krænkelse af rettigheder eller interesser i forbindelse med en persons personoplysninger og til at indbringe PIPC's afgørelser eller manglende handling for domstolene i henhold til lov om forvaltningssager. Registrerede har desuden adgang til retslig prøvelse i henhold til lov om forvaltningssager, hvis deres rettigheder eller interesser er blevet krænket som følge af den dataansvarliges disposition eller undladelse (f.eks. ulovlig indsamling af personoplysninger), eller til skadeserstatning efter lov om erstatning fra staten. Disse prøvelsesmekanismer er tilgængelige både i tilfælde af mulige overtrædelser af reglerne i specifikke love, der fastsætter begrænsninger og garantier for indsamling af personoplysninger, såsom den nationale sikkerhedslovgivning, og i PIPA.

En EU-borger kan indgive en klage til PIPC via sin nationale databeskyttelsesmyndighed, og PIPC underretter den pågældende via den nationale databeskyttelsesmyndighed, når undersøgelsen og den korrigerende foranstaltning (hvis det er relevant) er afsluttet.

BILAG II

18. maj 2021

Hans Excellence Didier Reynders, kommissær for retlige anliggender i Europa-Kommissionen

Deres Excellence

Jeg glæder mig over de konstruktive drøftelser mellem Korea og Kommissionen, der har til formål at skabe rammerne for overførsel af personoplysninger fra EU til Korea.

Efter anmodningen fra Kommissionen til Koreas regering sender jeg hermed et dokument, der giver et overblik over de retlige rammer for de koreanske myndigheders adgang til oplysninger.

Dette dokument vedrører mange ministerier og myndigheder i Korea, og for så vidt angår dokumentets indhold er de relevante ministerier og myndigheder (kommissionen for beskyttelse af personoplysninger, justitsministeriet, den nationale efterretningstjeneste, den nationale menneskerettighedskommission i Korea, det nationale center for terrorbekæmpelse, Koreas finansielle efterretningsenhed) ansvarlige for de passager, der falder inden for deres respektive kompetenceområder. De relevante ministerier og myndigheder er anført nedenfor.

Kommissionen for beskyttelse af personoplysninger modtager alle spørgsmål vedrørende dette dokument og koordinerer besvarelserne fra de relevante ministerier og myndigheder.

Jeg håber, at dette dokument vil være nyttigt med henblik på Europa-Kommissionens beslutningstagning.

Jeg sætter pris på det store bidrag, De har ydet i dette spørgsmål.

Med venlig hilsen

윤 종 인

Yoon Jong In
Formand for kommissionen for beskyttelse af personoplysninger

Dette dokument er udarbejdet af kommissionen for beskyttelse af personoplysninger og følgende berørte ministerier og myndigheder:

박 지 원

Park Jie Won
Formand (chef) for den nationale efterretningstjeneste

이 정 수

Lee Jung Soo
Generaldirektør, justitsministeriet

Choi Young Ae
Formand for den nationale menneskerettighedskommission i Korea

Kim Hyuck Soo
Direktør for det nationale center for terrorbekæmpelse

Kim, Jeong Kag
Kommissær, Koreas finansielle efterretningsenhed

Retlige rammer for de koreanske offentlige myndigheders indsamling og anvendelse af personoplysninger med henblik på retshåndhævelse og til nationale sikkerhedsformål

Følgende dokument indeholder et overblik over de retlige rammer for koreanske offentlige myndigheders indsamling og anvendelse af personoplysninger med henblik på strafferetlig håndhævelse og til nationale sikkerhedsformål (herefter »*myndighedsadgang*«), navnlig med hensyn til det relevante retsgrundlag, gældende betingelser (begrænsninger) og garantier samt uafhængigt tilsyn og individuel prøvelsesadgang.

1. DE GENERELLE RETSPRINCIPPER, DER ER RELEVANTE FOR MYNDIGHEDSADGANG

1.1. Forfatningsmæssige rammer

I Republikken Koreas forfatning fastsættes retten til privatlivets fred generelt (artikel 17) og mere specifikt retten til privatlivets fred i forbindelse med korrespondance (artikel 18). Det er statens pligt at garantere disse grundlæggende rettigheder ([1]). Det fastsættes endvidere i forfatningen, at borgernes rettigheder og friheder kun kan begrænses ved lov, og når det er nødvendigt af hensyn til den nationale sikkerhed eller opretholdelsen af lov og orden og den offentlige velfærd ([2]). Selv om der indføres sådanne begrænsninger, må de ikke berøre frihedens eller rettighedens væsentligste indhold ([3]). De koreanske domstole har anvendt disse bestemmelser i sager vedrørende statslig indgriben i privatlivets fred. Højesteret fandt f.eks., at overvågningen af civile krænkede den grundlæggende ret til privatlivets fred, og understregede, at borgerne har »ret til selvbestemmelse over personoplysninger« ([4]). I en anden sag fastslog forfatningsdomstolen, at retten til privatlivets fred er en grundlæggende rettighed, der yder beskyttelse mod statslig indgriben i og overvågning af borgernes privatliv ([5]).

Den koreanske forfatning garanterer endvidere, at ingen må anholdes, tilbageholdes, ransages eller afhøres, og at ingen genstande må beslaglægges, medmindre andet er fastsat ved lov ([6]). Ransagninger og beslaglæggelser kan endvidere kun foretages på grundlag af en retskendelse efter anmodning fra en anklager og under overholdelse af princippet om en retfærdig rettergang ([7]). Under ekstraordinære omstændigheder, dvs. hvor den mistænkte for forbrydelsen pågribes på fersk gerning (flagrante delicto), eller hvor der er risiko for, at en person, der mistænkes for at have begået en forbrydelse, der kan straffes med fængsel på tre år eller mere, kan undslippe eller ødelægge bevismateriale, kan efterforskningsmyndighederne foretage ransagning eller beslaglæggelse uden en kendelse, og de skal efterfølgende anmode om en kendelse ([8]). Disse generelle principper er videreudviklet i specifikke love om strafferetspleje og beskyttelse af kommunikation (se nedenfor for en detaljeret oversigt).

Med hensyn til udenlandske statsborgere bestemmer forfatningen, at deres status er garanteret i overensstemmelse med folkeretten og internationale traktater ([9]). En række internationale aftaler, som Korea er part i, garanterer retten til privatlivets fred, herunder den internationale konvention om borgerlige og politiske rettigheder (artikel 17), konventionen om rettigheder for personer med handicap (artikel 22) og konventionen om barnets rettigheder (artikel 16). Selv om der i forfatningen i princippet henvises til »*borgernes*« rettigheder, har forfatningsdomstolen desuden fastslået, at også udenlandske statsborgere har grundlæggende rettigheder ([10]). Domstolen har navnlig fastslået, at beskyttelsen af værdighed og en persons værdi som menneske samt retten til at søge lykke er rettigheder, der tilkommer

([1]) Artikel 10 i Republikken Koreas forfatning, bekendtgjort den 17. juli 1948 (»forfatningen«).
([2]) Forfatningens artikel 37, stk. 2.
([3]) Forfatningens artikel 37, stk. 2.
([4]) Den koreanske højesterets afgørelse nr. 96DA42789 af 24. juli 1998.
([5]) Forfatningsdomstolens afgørelse nr. 2002Hun-Ma51 af 30. oktober 2003. På samme måde præciserede forfatningsdomstolen i afgørelse 99Hun-Ma513 og 2004Hun-Ma190 (konsolideret) af 26. maj 2005, at »*retten til at kontrollere egne personoplysninger er en ret, der tilkommer den person, som er genstand for oplysningerne, til selv at afgøre, til hvem eller af hvem og i hvilket omfang vedkommendes oplysninger må videregives eller anvendes. Det er en grundlæggende ret, selv om den ikke er specificeret i forfatningen, der skal beskytte den personlige beslutningsfrihed mod risikoen forbundet med udvidelsen af statens funktioner og informations- og kommunikationsteknologien.*«
([6]) Forfatningens artikel 12, stk. 1, første punktum.
([7]) Forfatningens artikel 16 og artikel 12, stk. 3.
([8]) Forfatningens artikel 12, stk. 3.
([9]) Forfatningens artikel 6, stk. 2.
([10]) Forfatningsdomstolens afgørelse nr. 93Hun-MA120 af 29. december 1994. Se også f.eks. forfatningsdomstolens afgørelse nr. 2014Hun-Ma346 af 31. maj 2018, hvori domstolen fastslog, at en i lufthavnen tilbageholdt sudanesisk statsborgers forfatningsret til at modtage juridisk bistand var blevet krænket. I en anden sag fandt forfatningsdomstolen, at friheden til at vælge ens lovlige arbejdsplads hænger tæt sammen med retten til at stræbe efter lykke samt menneskelig værdighed og værdi og derfor ikke kun er forbeholdt statsborgere, men også kan sikres udlændinge, der er lovligt beskæftiget i Republikken Korea (forfatningsdomstolens afgørelse nr. 2007Hun-Ma1083 af 29. september 2011).

ethvert menneske og ikke blot statsborgere ([11]). Domstolen præciserede også, at retten til at kontrollere egne oplysninger betragtes som en grundlæggende rettighed, der bygger på retten til værdighed og stræben efter lykke og retten til privatlivets fred ([12]). Selv om hidtidig retspraksis ikke specifikt har behandlet ikkekoreanske statsborgeres ret til privatlivets fred, er det derfor almindeligt anerkendt blandt akademikere, at »*menneskerettighederne*« er fastsat i forfatningens artikel 12-22 (som omfatter retten til privatlivets fred og personlig frihed).

Endelig sikrer forfatningen også retten til at kræve en rimelig erstatning fra offentlige myndigheder ([13]). På grundlag af lov om forfatningsdomstolen kan enhver, hvis grundlæggende forfatningssikrede rettigheder krænkes som følge af udøvelsen af offentlig myndighed (bortset fra domstolsafgørelser), desuden indgive en forfatningsmæssig klage til forfatningsdomstolen ([14]).

1.2. **Generelle databeskyttelsesregler**

Den generelle databeskyttelseslov i Republikken Korea, lov om beskyttelse af personoplysninger (»*PIPA*«), finder anvendelse på både den private og den offentlige sektor. Med hensyn til offentlige myndigheder henvises der i PIPA specifikt til forpligtelsen til at formulere politikker til forebyggelse af »*misbrug og forkert anvendelse af personoplysninger, indiskret overvågning og sporing mv. og til styrkelse af den enkeltes værdighed og ret til privatlivets fred*« ([15]).

Behandlingen af personoplysninger med henblik på retshåndhævelse er underlagt alle kravene i PIPA. Dette betyder f. eks., at strafferetlige håndhævelsesmyndigheder skal overholde forpligtelserne vedrørende lovlig behandling, dvs. anvende et af retsgrundlagene i PIPA til indsamling, anvendelse eller videregivelse af personoplysninger (artikel 15-18 i PIPA) samt principperne om formålsbegrænsning (artikel 3, stk. 1 og 2, i PIPA), proportionalitet og dataminimering (artikel 3, stk. 1 og 6, i PIPA), opbevaringsbegrænsning (artikel 21 i PIPA), datasikkerhed, herunder anmeldelse af brud på datasikkerheden (artikel 3, stk. 4, artikel 29 og 34 i PIPA) og gennemsigtighed (artikel 3, stk. 1 og 5, artikel 20, 30 og 32 i PIPA). Der gælder særlige garantier for følsomme oplysninger (artikel 23 i PIPA). Desuden kan enkeltpersoner i henhold til artikel 3, stk. 5, og artikel 4 i PIPA samt artikel 35 til 39-2 i PIPA udøve deres ret til indsigt, berigtigelse, sletning og suspension over for de retshåndhævende myndigheder.

Selv om PIPA derfor finder fuldt ud anvendelse på behandling af personoplysninger med henblik på strafferetlig håndhævelse, indeholder den en undtagelse i forbindelse med behandling af personoplysninger til nationale sikkerhedsformål. I henhold til artikel 58, stk. 1, nr. 2, i PIPA finder artikel 15-50 i PIPA ikke anvendelse på personoplysninger, der indsamles eller udbedes med henblik på analyse af oplysninger vedrørende den nationale sikkerhed ([16]). Omvendt finder kapitel I (almindelige bestemmelser), kapitel II (fastlæggelse af politikker for beskyttelse af personoplysninger mv.), kapitel VIII (kollektive søgsmål vedrørende dataovertrædelse), kapitel IX (supplerende bestemmelser) og kapitel X (sanktionsbestemmelser) fortsat anvendelse. Dette omfatter de generelle databeskyttelsesprincipper, der er fastsat i artikel 3 (principper for beskyttelse af personoplysninger) og de individuelle rettigheder, der er sikret ved artikel 4 i PIPA (registreredes rettigheder). Det betyder, at de vigtigste principper og rettigheder også er garanteret på dette område. Desuden fastsættes det i artikel 58, stk. 4, i PIPA, at sådanne oplysninger skal behandles i mindst muligt omfang for at nå det tilsigtede formål og ikke længere end nødvendigt. Desuden kræves det, at den persondataansvarlige træffer de nødvendige foranstaltninger til at garantere en sikker dataforvaltning og korrekt behandling såsom tekniske, ledelsesmæssige og fysiske garantier samt foranstaltninger til korrekt behandling af individuelle klager.

I meddelelse nr. 2021-1 om supplerende regler for fortolkning og anvendelse af lov om beskyttelse af personoplysninger har kommissionen for beskyttelse af personoplysninger (»*PIPC*« eller »beskyttelseskommissionen«) yderligere præciseret, hvordan PIPA finder anvendelse på behandling af personoplysninger til nationale sikkerhedsformål i lyset af denne delvise undtagelse ([17]). Dette omfatter navnlig den enkeltes rettigheder (indsigt, berigtigelse, suspension og sletning) og begrundelserne samt begrænsninger for eventuelle begrænsninger heraf. Ifølge meddelelsen afspejler anvendelsen af de grundlæggende principper, rettigheder og forpligtelser i PIPA i forbindelse med behandling af personoplysninger

([11]) Forfatningsdomstolens afgørelse nr. 99HeonMa494 af 29. november 2001.
([12]) Jf. f.eks. forfatningsdomstolens afgørelse nr. 99HunMa513.
([13]) Forfatningens artikel 29, stk. 1.
([14]) Artikel 68, stk. 1, i lov om forfatningsdomstolen.
([15]) Artikel 5, stk. 1, i PIPA.
([16]) Artikel 58, stk. 1, nr. 2, i PIPA.
([17]) PIPC-meddelelse nr. 2021-1 om supplerende regler for fortolkning og anvendelse af lov om beskyttelse af personoplysninger, afsnit III, 6.

til nationale sikkerhedsformål de garantier, der er nedfældet i forfatningen, for beskyttelse af den enkeltes ret til at kontrollere sine egne personoplysninger. Enhver begrænsning af denne ret, f.eks. når det er nødvendigt for at beskytte statens sikkerhed, kræver en afvejning af den enkeltes rettigheder og interesser i forhold til den relevante offentlige interesse og må ikke berøre rettighedens væsentligste indhold (forfatningens artikel 37, stk. 2).

2. MYNDIGHEDSADGANG MED HENBLIK PÅ RETSHÅNDHÆVELSE

2.1. **Kompetente offentlige retshåndhævende myndigheder**

På grundlag af strafferetsplejeloven (»*CPA*«), lov om beskyttelse af privatlivets fred i forbindelse med kommunikation (»*CPPA*«) og telekommunikationsloven (»*TBA*«) kan politiet, anklagere og domstolene indsamle personoplysninger med henblik på strafferetlig håndhævelse. I det omfang den nationale efterretningstjeneste (»*NIS*«) også tildeles denne beføjelse i lov om den nationale efterretningstjeneste, skal efterretningstjenesten overholde ovennævnte love ([18]). Endelig udgør lov om indberetning og anvendelse af specifikke oplysninger om finansielle transaktioner (»ARUSFTI«) et retsgrundlag for, at finansielle institutioner kan videregive oplysninger til Koreas finansielle efterretningsenhed (»KOFIU«) med henblik på at forebygge hvidvaskning af penge og finansiering af terrorisme. Denne specialiserede enhed kan til gengæld videregive sådanne oplysninger til de retshåndhævende myndigheder. Disse oplysningsforpligtelser gælder dog kun for dataansvarlige, der behandler personlige kreditoplysninger i henhold til lov om kreditoplysninger og er underlagt kommissionen for finansielle tjenesteydelsers tilsyn. Da sådanne dataansvarliges behandling af personlige kreditoplysninger er udelukket fra anvendelsesområdet for afgørelsen om tilstrækkeligheden af beskyttelsesniveauet, er de begrænsninger og garantier, der gælder i henhold til ARUSFTI, ikke beskrevet nærmere i dette dokument.

2.2. **Retsgrundlag og begrænsninger**

CPA (se 2.2.1), CPPA (se 2.2.2) og telekommunikationsloven (se 2.2.3) danner retsgrundlag for indsamling af personoplysninger med henblik på retshåndhævelse og fastsætter de gældende begrænsninger og garantier.

2.2.1. *Ransagning og beslaglæggelse*

2.2.1.1. Retsgrundlag

Anklagere og kriminalpolitiet må kun inspicere genstande, ransage personer eller beslaglægge genstande, 1) hvis en person mistænkes for at have begået en forbrydelse (den mistænkte for forbrydelsen), 2) hvis det er nødvendigt for efterforskningen, og 3) hvis de genstande, der skal inspiceres, de personer, der skal ransages, og alle beslaglagte genstande anses for at være forbundet med sagen ([19]). Domstolene kan ligeledes foretage ransagning og beslaglægge genstande, der skal anvendes som bevismateriale eller kan konfiskeres, så længe sådanne genstande eller personer anses for at være forbundet med en specifik sag ([20]).

2.2.1.2. Begrænsninger og garantier

Som en generel forpligtelse skal anklagere og kriminalpolitiet respektere den mistænkte for forbrydelsens og enhver anden berørt persons menneskerettigheder ([21]). Desuden må der kun træffes obligatoriske foranstaltninger for at nå formålet med efterforskningen, hvis det er udtrykkeligt fastsat i CPA, og kun i nødvendigt omfang ([22]).

Politiets og anklagerens ransagninger, inspektioner eller beslaglæggelser som led i en strafferetlig efterforskning må kun finde sted på grundlag af en retskendelse ([23]). Den myndighed, der anmoder om en kendelse, skal fremlægge dokumentation for, at der er begrundet mistanke om, at en person har begået en forbrydelse, at ransagningen, inspektionen eller beslaglæggelsen er nødvendig, og at de relevante genstande, der skal beslaglægges, findes ([24]). Kendelsen skal bl.a. indeholde navnet på den mistænkte for forbrydelsen og en beskrivelse af den strafbare handling, det sted, den person eller de genstande, der skal ransages, eller de genstande, der skal beslaglægges, udstedelsesdatoen og den faktiske anvendelsesperiode ([25]). Når der foretages ransagninger og beslaglæggelser som led i verserende retssager på anden måde end i offentligt retsmøde, skal der ligeledes indhentes en retskendelse på forhånd ([26]). Den pågældende person og dennes forsvarer underrettes forud for ransagningen eller beslaglæggelsen og kan være til stede, når kendelsen fuldbyrdes ([27]).

([18]) Jf. artikel 3 i NIS-loven (lov nr. 12948), der vedrører strafferetlig efterforskning af visse former for kriminalitet såsom oprør, opstand og kriminalitet i forbindelse med den nationale sikkerhed (f.eks. spionage). Procedurerne i CPA vedrørende ransagning og beslaglæggelse finder anvendelse i denne sammenhæng, og CPPA regulerer indsamlingen af kommunikationsdata (jf. del 3 om bestemmelserne om adgang til kommunikation til nationale sikkerhedsformål).
([19]) Artikel 215, stk. 1 og 2, i CPA.
([20]) Artikel 106, stk. 1, og artikel 107 og 109 i CPA.
([21]) Artikel 198, stk. 2, i CPA.
([22]) Artikel 199, stk. 1, i CPA.
([23]) Artikel 215, stk. 1 og 2, i CPA.
([24]) Artikel 108, stk. 1, i strafferetsplejeloven.
([25]) Artikel 114, stk. 1, i CPA sammenholdt med artikel 219 i CPA.
([26]) Artikel 113 i CPA.
([27]) Artikel 121 og 122 i CPA.

Når der foretages ransagning eller beslaglæggelse, og den genstand, der skal ransages, er en diskette eller et andet datalagringsmedium, er det i princippet kun oplysningerne (i kopi eller udskrevet), der beslaglægges, og ikke hele mediet ([28]). Datalagringsmediet kan kun beslaglægges, hvis det anses for at være stort set umuligt at udskrive eller kopiere de krævede oplysninger særskilt, eller hvis det anses for at være praktisk umuligt at opfylde formålet med ransagningen på anden vis ([29]). Den pågældende person skal straks underrettes om beslaglæggelsen ([30]). Der er ingen undtagelser fra dette underretningskrav i CPA.

Ransagninger, inspektioner og beslaglæggelser uden en kendelse må kun finde sted i begrænsede situationer. For det første er dette tilfældet, når det er umuligt at indhente en kendelse på grund af situationens hastende karakter på gerningsstedet ([31]). Der skal dog efterfølgende straks indhentes en kendelse ([32]). For det andet kan der foretages ransagninger og inspektioner på stedet uden en kendelse i forbindelse med anholdelsen eller tilbageholdelsen af den mistænkte for forbrydelsen ([33]). Endelig kan en anklager eller kriminalpolitiet beslaglægge en genstand uden en kendelse, hvis genstanden er blevet bortsmidt af den mistænkte for forbrydelsen eller tredjemand eller er blevet frivilligt udleveret ([34]).

Bevismateriale, der er fremskaffet i strid med CPA, betragtes som uantageligt ([35]). I henhold til straffeloven straffes ulovlig ransagning af personer eller en persons bopæl, bevogtede bygning, konstruktion, bil, skib, fly eller beboet lokale desuden med fængsel i op til tre år ([36]). Denne bestemmelse finder derfor også anvendelse, når genstande såsom datalagringsudstyr beslaglægges under en ulovlig ransagning.

2.2.2. *Indsamling af kommunikationsdata*

2.2.2.1. Retsgrundlag

Indsamlingen af kommunikationsdata er reguleret ved en særlig lov, CPPA. CPPA forbyder navnlig enhver censur af post, aflytning af telekommunikation, videregivelse af kommunikationsbekræftelsesdata eller registrering eller lytning til private samtaler, undtagen på grundlag af CPA, CPaPA eller lov om militærdomstolen ([37]). Begrebet »*kommunikation*« som omhandlet i CPPA omfatter både almindelig post og telekommunikation ([38]). I denne forbindelse skelner CPPA mellem »*kommunikationsbegrænsende foranstaltninger*« ([39]) og indsamling af »*kommunikationsbekræftelsesdata*«.

Begrebet kommunikationsbegrænsende foranstaltninger omfatter »censur«, dvs. indsamling af indholdet af traditionel post, samt »aflytning«, dvs. direkte aflytning (indsamling eller optagelse) af indholdet af telekommunikation ([40]). Ved »kommunikationsbekræftelsesdata« forstås »*data om telekommunikationsregistreringer*«, herunder telekommunikationasdato, start- og sluttidspunkt, antal udgående og indgående opkald samt den anden parts abonnentnummer, hyppighed, logfiler om brugen af teletjenester og lokaliseringsdata (f.eks. fra transmissionstårne, hvor der modtages signaler) ([41]).

([28]) Artikel 106, stk. 3, i CPA.
([29]) Artikel 106, stk. 3, i CPA.
([30]) Artikel 219 i CPA sammenholdt med artikel 106, stk. 4, i CPA.
([31]) Artikel 216, stk. 3, i CPA.
([32]) Artikel 216, stk. 3, i CPA.
([33]) Artikel 216, stk. 1 og 2, i CPA.
([34]) Artikel 218 i CPA. For så vidt angår personoplysninger omfatter dette kun frivillig videregivelse fra den pågældende selv og ikke fra en persondataansvarlig, der er i besiddelse af sådanne oplysninger (hvilket ville kræve et specifikt retsgrundlag i lov om beskyttelse af personoplysninger). Frivilligt udleverede genstande antages kun som bevismateriale i retssager, hvis der ikke er nogen rimelig tvivl om udleveringens frivillige karakter, hvilket det påhviler anklageren at bevise. Jf. højesterets afgørelse 2013Do11233 af 10. marts 2016.
([35]) Artikel 308-2 i CPA.
([36]) Artikel 321 i straffeloven.
([37]) Artikel 3 i CPPA. Loven regulerer imidlertid indsamlingen af oplysninger om militærpersonel og kan kun finde anvendelse på civile i et begrænset antal tilfælde (f.eks. hvis militærpersonel og civile begår en forbrydelse sammen, eller hvis en person begår en forbrydelse mod militæret, kan der anlægges sag ved en militærdomstol, jf. artikel 2 i lov om militærdomstolen). De generelle bestemmelser om ransagning og beslaglæggelse svarer til bestemmelserne i CPA, jf. f.eks. artikel 146-149 og 153-156 i lov om militærdomstolen. F.eks. må postforsendelser kun indsamles, når det er nødvendigt for efterforskningen, og på grundlag af en kendelse fra militærdomstolen. I det omfang elektronisk kommunikation indsamles, finder begrænsningerne og garantierne i CPPA anvendelse.
([38]) Artikel 2, stk. 1, i CPPA: »*transmission eller modtagelse af alle former for lyd, ord, symboler eller billeder over ledningstråd, trådløst, fiberkabel eller andet elektromagnetisk system, herunder telefon, e-mail, medlemskabsinformationstjeneste, telefax og radiopersonsøgning*«.
([39]) Artikel 2, stk. 7, og artikel 3, stk. 2, i CPPA.
([40]) »Censur« defineres som »*åbning af post uden den pågældende parts samtykke eller indsamling af viden om, optagelse eller tilbageholdelse af dens indhold ved brug af andre midler*« (artikel 2, stk. 6, i CPPA). »Aflytning« defineres som »*indsamling eller optagelse af indholdet af telekommunikation ved at lytte til eller læse lyde, ord, symboler eller billeder i kommunikationen ved brug af elektroniske og mekaniske anordninger uden den pågældende parts samtykke eller gribe ind i deres transmission og modtagelse*« (artikel 2, stk. 7, i CPPA).
([41]) Artikel 2, stk. 11, i CPPA.

CPPA fastsætter begrænsninger og garantier for indsamlingen af begge typer data, og manglende overholdelse af flere af disse krav straffes med strafferetlige sanktioner ([42]).

2.2.2.2. Begrænsninger og garantier for indsamling af indholdet af kommunikation (kommunikationsbegrænsende foranstaltninger)

Indsamlingen af indholdet af kommunikation må kun ske som et supplerende middel til at lette en strafferetlig efterforskning (dvs. som en sidste udvej), og der skal gøres en indsats for at minimere indgrebet i borgernes ret til kommunikationshemmelighed ([43]). I overensstemmelse med dette generelle princip må kommunikationsbegrænsende foranstaltninger kun anvendes, hvis det er vanskeligt at forhindre, at der begås en forbrydelse, at anholde en kriminel person eller at indsamle bevismateriale på anden vis ([44]). De retshåndhævende myndigheder, der indsamler indholdet af kommunikation, skal straks ophøre hermed, når fortsat adgang ikke længere anses for nødvendig, hvorved det sikres, at krænkelsen af privatlivets fred i forbindelse med kommunikation begrænses mest muligt ([45]).

Kommunikationsbegrænsende foranstaltninger må kun anvendes, hvis der er vægtige grunde til at formode, at visse former for grov kriminalitet, der er specifikt anført i CPPA, planlægges, begås eller er blevet begået. Dette omfatter kriminalitet såsom oprør, narkokriminalitet, sprængstofkriminalitet samt kriminalitet i forbindelse med den nationale sikkerhed, diplomatiske forbindelser eller militærbaser og -anlæg ([46]). Den kommunikationsbegrænsende foranstaltning skal være rettet mod specifikke brevforsendelser eller specifik telekommunikation, der sendes eller modtages af den mistænkte, eller brevforsendelser eller telekommunikation, der sendes eller modtages af den mistænkte i en bestemt periode ([47]).

Selv når disse krav er opfyldt, kan indsamlingen af indholdsdata kun finde sted på grundlag af en retskendelse. En anklager kan navnlig anmode retten om at tillade indsamling af indholdsdata om den mistænkte eller den efterforskede person ([48]). På samme måde kan kriminalpolitiet anmode en anklager om tilladelse, og anklageren kan herefter anmode retten om en kendelse ([49]). En anmodning om en kendelse skal fremsættes skriftligt og indeholde specifikke elementer. Den skal navnlig indeholde en beskrivelse af 1) de vægtige grunde til at formode, at en af de anførte former for kriminalitet planlægges, begås eller er blevet begået, samt eventuelt materiale, der godtgør, at der umiddelbart er et grundlag for mistanken, 2) de kommunikationsbegrænsende foranstaltninger og deres mål, omfang, formål og varighed og af 3) det sted, hvor foranstaltningerne vil blive gennemført, og hvordan de vil blive gennemført ([50]).

Hvis de retlige krav er opfyldt, kan retten give skriftlig tilladelse til at gennemføre kommunikationsbegrænsende foranstaltninger rettet mod den mistænkte eller den efterforskede person ([51]). I denne kendelse angives de forskellige typer foranstaltninger samt deres mål, omfang, varighed, gennemførelsessted og gennemførelsesmetode ([52]).

Kommunikationsbegrænsende foranstaltninger må kun gennemføres i en periode på to måneder ([53]). Hvis formålet med foranstaltningerne nås tidligere inden for denne frist, skal foranstaltningerne straks bringes til ophør. Hvis de nødvendige betingelser derimod stadig er opfyldt, kan der inden for fristen på to måneder indgives en anmodning om forlængelse af de kommunikationsbegrænsende foranstaltningers varighed. En sådan anmodning skal indeholde materiale, der godtgør, at der umiddelbart er grundlag for at forlænge foranstaltningerne ([54]). Den forlængede periode må ikke overstige et år eller tre år for visse former for særlig grov kriminalitet (f.eks. kriminalitet i forbindelse med oprør, aggression udefra og den nationale sikkerhed mv.) ([55]).

De retshåndhævende myndigheder kan tvinge kommunikationsoperatører til at bistå ved at give dem rettens skriftlige tilladelse ([56]). Kommunikationsoperatører skal samarbejde og opbevare den modtagne tilladelse ([57]). De kan nægte at samarbejde, hvis oplysningerne om den overvågede person angivet i rettens skriftlige tilladelse (f.eks. personens telefonnummer) er ukorrekte. De må desuden under alle omstændigheder ikke videregive adgangskoder, der anvendes til telekommunikation ([58]).

([42]) Artikel 16 og 17 i CPPA. Dette gælder f.eks. indsamling uden en kendelse, manglende registrering, undladelse af at indstille indsamlingen, når en nødsituationen er ophørt, eller manglende underretning af den pågældende person.
([43]) Artikel 3, stk. 2, i CPPA.
([44]) Artikel 5, stk. 1, i CPPA.
([45]) Artikel 2 i CPPA-gennemførelsesdekretet.
([46]) Artikel 5, stk. 1, i CPPA.
([47]) Artikel 5, stk. 2, i CPPA.
([48]) Artikel 6, stk. 1, i CPPA.
([49]) Artikel 6, stk. 2, i CPPA.
([50]) Artikel 6, stk. 4, i CPPA og artikel 4, stk. 1, i CPPA-gennemførelsesdekretet.
([51]) Artikel 6, stk. 5, og artikel 6, stk. 8, i CPPA.
([52]) Artikel 6, stk. 6, i CPPA.
([53]) Artikel 6, stk. 7, i CPPA.
([54]) Artikel 6, stk. 7, i CPPA.
([55]) Artikel 6, stk. 8, i CPPA.
([56]) Artikel 9, stk. 2, i CPPA.
([57]) Artikel 15-2 i CPPA og artikel 12 i CPPA-gennemførelsesdekretet.
([58]) Artikel 9, stk. 4, i CPPA.

Enhver, der gennemfører kommunikationsbegrænsende foranstaltninger, eller som anmodes om at samarbejde, skal føre fortegnelser med angivelse af formålene med foranstaltningerne, gennemførelsen, datoen for indledningen af samarbejdet og målet ([59]). Retshåndhævende myndigheder, der gennemfører kommunikationsbegrænsende foranstaltninger, skal også føre fortegnelser med nærmere oplysninger og opnåede resultater ([60]). Kriminalpolitiet skal give disse oplysninger i form af en rapport til anklageren ved afslutningen af en efterforskning ([61]).

Når en anklager rejser tiltale i en sag, hvor der blev anvendt kommunikationsbegrænsende foranstaltninger, eller udsteder en afgørelse om ikke at rejse tiltale eller anholde den pågældende person (dvs. at der ikke blot er tale om en udsættelse af retsforfølgelsen), skal anklageren underrette den person, der er underlagt de kommunikationsbegrænsende foranstaltninger, om, at der er gennemført kommunikationsbegrænsende foranstaltninger, og om gennemførelsesmyndigheden og gennemførelsesperioden. Underretningen skal ske skriftligt senest 30 dage efter afgørelsen ([62]). Underretningen kan udsættes, hvis den sandsynligvis vil bringe den nationale sikkerhed i alvorlig fare eller forstyrre den offentlige orden, eller hvis den sandsynligvis vil påføre andres liv og legeme fysisk skade ([63]). Hvis anklageren eller kriminalpolitiet ønsker at udsætte underretningen, skal de indhente godkendelse fra chefen for distriktsadvokaturen ([64]). Underretningen skal ske senest 30 dage efter, at årsagerne til udsættelsen ikke længere gør sig gældende ([65]).

CPPA fastsætter også en særlig procedure for indsamling af indholdet af kommunikation i nødsituationer. De retshåndhævende myndigheder kan navnlig indsamle indholdet af kommunikation, hvis der er en overhængende fare for planlægning eller gennemførelse af organiseret kriminalitet eller anden grov kriminalitet, som kan forårsage direkte dødsfald eller alvorlig personskade, og der foreligger en nødsituation, som gør det umuligt at følge den almindelige procedure (som beskrevet ovenfor) ([66]). I en sådan nødsituation kan politiet eller anklageren træffe kommunikationsbegrænsende foranstaltninger uden en forudgående retskendelse, men skal anmode om en retskendelse umiddelbart efter gennemførelsen. Hvis det retshåndhævende organ ikke indhenter retskendelsen inden for 36 timer fra tidspunktet for iværksættelse af hasteforanstaltningerne, skal indsamlingen straks indstilles, typisk efterfulgt af tilintetgørelse af de indsamlede oplysninger ([67]). Politiet gennemfører nødovervågning under kontrol af en anklager, og hvis det ikke er muligt at modtage instrukser fra anklageren på forhånd, fordi det er nødvendigt at handle hurtigt, skal politiet indhente anklagerens godkendelse umiddelbart efter påbegyndelsen af overvågningen ([68]). Reglerne om underretning af den berørte person som beskrevet ovenfor finder også anvendelse på indsamlingen af indholdet af kommunikation i nødsituationer.

Indsamling af oplysninger i nødsituationer skal altid finde sted i overensstemmelse med en »*erklæring om censur/aflytning i nødsituationer*«, og den myndighed, der foretager indsamlingen, skal føre et register over alle hasteforanstaltninger ([69]). Anmodningen til en domstol om tilladelse til at træffe hasteforanstaltninger skal ledsages af et skriftligt dokument med angivelse af de nødvendige kommunikationsbegrænsende foranstaltninger, mål, omfang, varighed, gennemførelsessted, metode og en redegørelse for, hvordan de relevante kommunikationsbegrænsende foranstaltninger opfylder artikel 5, stk. 1, i CPPA ([70]), sammen med dokumentation.

Hvis hasteforanstaltningerne afsluttes inden for kort tid og uden en retskendelse (f.eks. hvis den mistænkte anholdes umiddelbart efter påbegyndelsen af aflytningen, som derfor stopper), indgiver chefen for den kompetente anklagemyndighed en meddelelse om hasteforanstaltninger til den kompetente ret ([71]). I meddelelsen angives formål, mål, omfang, varighed, gennemførelsessted og indsamlingsmetode samt begrundelsen for ikke at indgive en anmodning om en retskendelse ([72]). Denne meddelelse giver den modtagende ret mulighed for at undersøge, om indsamlingen er lovlig, og den skal indføres i et register over meddelelser om hasteforanstaltninger.

([59]) Artikel 9, stk. 3, i CPPA.
([60]) Artikel 18, stk. 1, i CPPA-gennemførelsesdekretet.
([61]) Artikel 18, stk. 2, i CPPA-gennemførelsesdekretet.
([62]) Artikel 9-2, stk. 1, i CPPA.
([63]) Artikel 9-2, stk. 4, i CPPA.
([64]) Artikel 9-2, stk. 5, i CPPA.
([65]) Artikel 9-2, stk. 6, i CPPA.
([66]) Artikel 8, stk. 1, i CPPA.
([67]) Artikel 8, stk. 2, i CPPA.
([68]) Artikel 8, stk. 3, i CPPA og artikel 16, stk. 3, i CPPA-gennemførelsesdekretet.
([69]) Artikel 8, stk. 4, i CPPA.
([70]) Der er således vægtige grunde til at formode, at visse former for grov kriminalitet planlægges, begås eller er blevet begået, og det er i praksis umuligt at forhindre, at der begås en forbrydelse, at anholde en kriminel person eller at indsamle bevismateriale på anden vis.
([71]) Artikel 8, stk. 5, i CPPA.
([72]) Artikel 8, stk. 6-7, i CPPA.

Som et generelt krav må indholdet af kommunikation, der erhverves via gennemførelse af kommunikationsbegrænsende foranstaltninger på grundlag af CPPA, kun anvendes til at efterforske, retsforfølge eller forebygge de specifikke former for kriminalitet, der er nævnt ovenfor, i disciplinærsager i forbindelse med denne kriminalitet, i forbindelse med et erstatningskrav rejst af en part i kommunikationen, eller hvor dette er tilladt i henhold til anden lovgivning ([73]).

Der gælder særlige garantier ved indsamling af telekommunikation, der overføres via internettet ([74]). Sådanne oplysninger må kun anvendes til at efterforske de former for grov kriminalitet, der er anført i artikel 5, stk. 1, i CPPA. For at kunne opbevare oplysningerne skal der indhentes godkendelse fra den domstol, der godkendte de kommunikationsbegrænsende foranstaltninger ([75]). En anmodning om opbevaring skal indeholde oplysninger om de kommunikationsbegrænsende foranstaltninger, et resumé af resultaterne af foranstaltningerne, begrundelsen for opbevaringen (sammen med dokumentation) og oplysninger om den telekommunikation, der skal opbevares ([76]). Hvis der ikke foreligger en sådan anmodning, skal den erhvervede telekommunikation slettes senest 14 dage efter udløbet af de kommunikationsbegrænsende foranstaltninger ([77]). Hvis en anmodning afvises, skal telekommunikationen tilintetgøres inden for syv dage ([78]). Hvis telekommunikationen slettes, skal der senest syv dage herefter indgives en rapport til den domstol, der godkendte de kommunikationsbegrænsende foranstaltninger, med angivelse af årsagerne til sletningen samt nærmere oplysninger og tidsplanen herfor.

Mere generelt vil oplysninger, der er indhentet ulovligt ved brug af kommunikationsbegrænsende foranstaltninger, ikke blive antaget som bevismateriale i retssager eller disciplinærsager ([79]). Endvidere forbyder CPPA enhver, der træffer kommunikationsbegrænsende foranstaltninger, at videregive fortrolige oplysninger, der er indhentet i forbindelse med gennemførelsen af sådanne foranstaltninger, og at anvende de indhentede oplysninger til skade for de af foranstaltningerne omfattede personers omdømme ([80]).

2.2.2.3. Begrænsninger og garantier for indsamling af kommunikationsbekræftelsesdata

På grundlag af CPPA kan de retshåndhævende myndigheder anmode teleoperatører om at fremlægge kommunikationsbekræftelsesdata, når det er nødvendigt for at gennemføre en efterforskning eller fuldbyrde en dom ([81]). I modsætning til hvad der er tilfældet ved indsamling af indholdsdata, er muligheden for at indsamle kommunikationsbekræftelsesdata ikke begrænset til visse specifikke former for kriminalitet. Som det er tilfældet med indholdsdata, kræver indsamling af kommunikationsbekræftelsesdata imidlertid forudgående skriftlig tilladelse fra en domstol på de samme betingelser som beskrevet ovenfor ([82]). Når hensynet til sagens hastende karakter gør det umuligt at indhente en retskendelse, kan kommunikationsbekræftelsesdata indsamles uden en kendelse, og kendelsen skal i så fald indhentes umiddelbart efter anmodningen om oplysningerne og meddeles teleudbyderen ([83]). Hvis der ikke efterfølgende indhentes en kendelse, skal de indsamlede oplysninger tilintetgøres ([84]).

Anklagere, kriminalpolitiet og domstolene skal føre fortegnelser over anmodninger om kommunikationsbekræftelsesdata ([85]). Desuden skal teleudbydere to gange om året aflægge rapport om videregivelsen af kommunikationsbekræftelsesdata til ministeriet for videnskab og IKT, og de skal opbevare optegnelser herom i syv år fra datoen for videregivelse af oplysningerne ([86]).

De berørte personer underrettes i princippet om, at der er indsamlet kommunikationsbekræftelsesdata ([87]). Tidspunktet for en sådan underretning afhænger af omstændighederne omkring efterforskningen ([88]). Når der er truffet afgørelse om (ikke) at retsforfølge, skal underretningen ske senest 30 dage herefter. Hvis tiltalen derimod suspenderes, skal underretningen ske senest et år og 30 dage efter, at en sådan afgørelse er truffet. Underretningen skal under alle omstændigheder ske senest et år og 30 dage efter indsamlingen af oplysningerne.

Underretningen kan udsættes, hvis den sandsynligvis vil 1) bringe den nationale sikkerhed og den offentlige sikkerhed og orden i fare, 2) forårsage død eller legemsbeskadigelse, 3) hindre en retfærdig rettergang (f.eks. føre til ødelæggelse

([73]) Artikel 12 i CPPA.
([74]) Artikel 12-2 i CPPA.
([75]) Anklageren eller politiet, der gennemfører de kommunikationsbegrænsende foranstaltninger, skal udvælge den telekommunikation, der skal opbevares, senest 14 dage efter foranstaltningernes udløb og anmode om rettens godkendelse (i tilfælde af politiets indgriben skal anmodningen indgives til en anklager, som derefter indgiver anmodningen til retten), jf. artikel 12-2, stk. 1 og 2, i CPPA.
([76]) Artikel 12-2, stk. 3, i CPPA.
([77]) Artikel 12-2, stk. 5, i CPPA.
([78]) Artikel 12-2, stk. 5, i CPPA.
([79]) Artikel 4 i CPPA.
([80]) Artikel 11, stk. 2, i CPPA-gennemførelsesdekretet.
([81]) Artikel 13, stk. 1, i CPPA.
([82]) Artikel 13 og 6 i CPPA.
([83]) Artikel 13, stk. 2, i CPPA. Som det er tilfældet med hastende kommunikationsbegrænsende foranstaltninger, skal der udarbejdes et dokument med nærmere oplysninger om sagen (den mistænkte, de foranstaltninger, der skal træffes, den formodede forbrydelse samt sagens hastende karakter). Jf. artikel 37, stk. 5, i CPPA-gennemførelsesdekretet.
([84]) Artikel 13, stk. 3, i CPPA.
([85]) Artikel 13, stk. 5 og 6, i CPPA.
([86]) Artikel 13, stk. 7, i CPPA.
([87]) Jf. artikel 13-3, stk. 7, i CPPA sammenholdt med artikel 9-2 i CPPA.
([88]) Artikel 13-3, stk. 1, i CPPA.

af beviser eller trusler mod vidner) eller 4) ærekrænke den mistænkte, ofrene eller andre personer, der er indblandet i sagen, eller krænke deres privatliv ([89]). Underretning af en af ovennævnte årsager kræver tilladelse fra chefen for en kompetent distriktsadvokatur ([90]). Underretningen skal ske senest 30 dage efter, at årsagerne til udsættelsen ikke længere gør sig gældende ([91]).

Underrettede personer kan indgive en skriftlig anmodning til anklageren eller kriminalpolitiet vedrørende begrundelsen for indsamlingen af kommunikationsbekræftelsesdataene ([92]). I så fald skal anklageren eller kriminalpolitiet give en skriftlig begrundelse senest 30 dage efter modtagelsen af anmodningen, medmindre en af ovennævnte grunde (undtagelser for udsættelse af underretning) finder anvendelse ([93]).

2.2.3. *Teleoperatørers frivillige videregivelse af oplysninger*

I henhold til artikel 83, stk. 3, i TBA kan teleoperatører frivilligt imødekomme en anmodning (fremsat til støtte for en straffesag, efterforskning eller fuldbyrdelse af en dom) fra en domstol, en anklager eller chefen for et efterforskningsagentur om at videregive »*kommunikationsdata*«. I TBA omfatter »*kommunikationsdata*« brugernes navn, bopælsregistreringsnummer, adresse og telefonnummer, datoerne for brugernes tegning eller opsigelse af deres abonnement samt brugeridentifikationskoder (dvs. koder, der anvendes til at identificere den retmæssige bruger af computersystemer eller kommunikationsnet) ([94]). I forbindelse med TBA er det kun personer, som indgår aftaler om tjenester direkte med en koreansk teleudbyder, der betragtes som brugere ([95]). Som følge heraf vil de situationer, hvor EU-borgere, hvis oplysninger er blevet overført til Republikken Korea, vil blive betragtet som brugere i henhold til TBA, sandsynligvis være meget begrænsede, da disse personer normalt ikke indgår en direkte aftale med en koreansk teleoperatør.

Anmodningen om indhentning af kommunikationsdata på grundlag af TBA indgives skriftligt med angivelse af begrundelsen for anmodningen, linket til den relevante bruger og omfanget af de ønskede data ([96]). Hvis det på grund af sagens hastende karakter er umuligt at indgive en skriftlig anmodning, skal den skriftlige anmodning indgives, så snart der ikke længere er nogen begrundelse for sagens hastende karakter ([97]). Teleoperatører, der efterkommer anmodninger om videregivelse af kommunikationsdata, skal opbevare fortegnelser over videregivelsen af kommunikationsdata samt tilknyttet materiale såsom den skriftlige anmodning ([98]). Desuden skal teleoperatører to gange om året aflægge rapport om videregivelsen af kommunikationsdata til ministeriet for videnskab og IKT ([99]).

Teleoperatører er ikke forpligtet til at efterkomme anmodninger om videregivelse af kommunikationsdata på grundlag af TBA. Hver anmodning skal derfor vurderes af operatøren i lyset af de gældende databeskyttelseskrav i PIPA. Teleoperatører skal navnlig tage hensyn til den registreredes interesser og må ikke videregive oplysningerne, hvis dette sandsynligvis vil krænke den registreredes eller tredjemands interesser uretmæssigt ([100]). Desuden skal den berørte person i henhold til meddelelse nr. 2021-1 om supplerende regler for fortolkning og anvendelse af lov om beskyttelse af personoplysninger underrettes om videregivelsen. Under ekstraordinære omstændigheder kan underretningen udsættes, navnlig hvis og så længe underretningen vil bringe en igangværende strafferetlig efterforskning i fare eller sandsynligvis vil skade en anden persons liv eller legeme, hvis disse rettigheder eller interesser går klart forud for den registreredes rettigheder ([101]).

I 2016 bekræftede højesteret, at teleoperatørers frivillige videregivelse af kommunikationsdata uden en retskendelse på grundlag af TBA ikke i sig selv krænker brugeren af teletjenestens ret til selvbestemmelse over oplysninger. Samtidig præciserede højesteret, at der er tale om en sådan overtrædelse, hvis det er helt åbenbart, at den anmodende myndighed har misbrugt sin beføjelse til at anmode om videregivelse af kommunikationsdata og derved krænket den registreredes eller tredjemands interesser ([102]). Mere generelt skal enhver anmodning om frivillig fremlæggelse af oplysninger fra en retshåndhævende myndighed være i overensstemmelse principperne om lovlighed, nødvendighed og proportionalitet i den koreanske forfatning (artikel 12, stk. 1, og artikel 37, stk. 2).

([89]) Artikel 13-3, stk. 2, i CPPA.
([90]) Artikel 13-3, stk. 3, i CPPA.
([91]) Artikel 13-3, stk. 4, i CPPA.
([92]) Artikel 13-3, stk. 5, i CPPA.
([93]) Artikel 13-3, stk. 6, i CPPA.
([94]) Artikel 83, stk. 3, i TBA.
([95]) Artikel 2, stk. 9, i TBA.
([96]) Artikel 83, stk. 4, i TBA.
([97]) Artikel 83, stk. 4, i TBA.
([98]) Artikel 83, stk. 5, i TBA.
([99]) Artikel 83, stk. 6, i TBA.
([100]) Artikel 18, stk. 2, i PIPA.
([101]) PIPC-meddelelse nr. 2021-1 om supplerende regler for fortolkning og anvendelse af lov om beskyttelse af personoplysninger, afsnit III, 2, nr. iii).
([102]) Højesterets afgørelse nr. 2012Da105482 af 10. marts 2016.

2.3. **Tilsyn**

Tilsynet med de strafferetlige håndhævelsesmyndigheder varetages ved brug af forskellige mekanismer, både internt og via eksterne organer.

2.3.1. *Selvrevision*

I overensstemmelse med lov om revisioner i den offentlige sektor tilskyndes de offentlige myndigheder til at oprette et internt selvrevisionsorgan, der bl.a. har til opgave at udføre legalitetskontrol ([103]). Lederne af sådanne revisionsorganer skal i videst muligt omfang garanteres uafhængighed ([104]). Mere specifikt hentes de uden for den relevante myndighed (f. eks. tidligere dommere, professorer) og udnævnes for en periode på to til fem år og kan kun afsættes af velbegrundede årsager (f.eks. hvis de ikke kan varetage deres opgaver på grund af psykisk eller fysisk sygdom, eller hvis de er genstand for disciplinære sanktioner) ([105]). Revisorer udnævnes ligeledes på grundlag af særlige betingelser, der er fastsat i loven ([106]). Revisionsrapporter kan omfatte henstillinger eller anmodninger om erstatning eller berigtigelse samt irettesættelser og henstillinger eller anmodninger om disciplinære foranstaltninger ([107]). De meddeles lederen af den offentlige myndighed, der er genstand for revisionen, samt revisions- og inspektionsudvalget (jf. afsnit 2.3.2) senest 60 dage efter revisionens afslutning ([108]). Den pågældende myndighed skal gennemføre de nødvendige foranstaltninger og aflægge rapport om resultaterne til revisions- og inspektionsudvalget ([109]). Desuden stilles revisionsresultaterne generelt til rådighed for offentligheden ([110]). Nægtelse eller hindring af selvrevision straffes med administrative bøder ([111]). På det strafferetlige område har det nationale politiagentur indført et generalinspektørsystem til håndtering af interne revisioner, herunder mulige krænkelser af menneskerettighederne, for at overholde ovennævnte lovgivning ([112]).

2.3.2. *Revisions- og inspektionsudvalget*

Revisions- og inspektionsudvalget (»*BAI*«) kan inspicere offentlige myndigheders aktiviteter og på grundlag af sådanne inspektioner udstede henstillinger, anmode om disciplinære foranstaltninger eller indgive en anmeldelse ([113]). BAI er oprettet under Republikken Koreas præsident, men varetager sine opgaver uafhængigt ([114]). I henhold til lov om oprettelse af BAI skal BAI desuden have størst mulig uafhængighed med hensyn til udnævnelse, afskedigelse og organisation af sit personale og udarbejdelse af sit budget ([115]). Formanden for BAI udnævnes af præsidenten med nationalforsamlingens samtykke ([116]). De seks resterende kommissærer udnævnes af præsidenten efter indstilling fra formanden for en fireårig periode ([117]). Kommissærer (herunder formanden) skal opfylde specifikke lovbestemte kvalifikationskriterier ([118]) og kan kun afsættes i tilfælde af forfald, fængselsstraf eller manglende evne til at varetage deres opgaver på grund af langvarig psykisk eller fysisk sygdom ([119]). Kommissærer må desuden ikke deltage i politiske aktiviteter og sideløbende bestride hverv i nationalforsamlingen, forvaltningsorganer, organisationer, der er underlagt BAI's revision og inspektion, eller andre lønnede hverv eller stillinger ([120]).

BAI foretager en generel revision en gang om året, men kan også foretage specifikke revisioner af spørgsmål af særlig interesse. BAI kan anmode om fremlæggelse af dokumenter under en inspektion og indkalde enkeltpersoner ([121]). Som led i en revision undersøger BAI statens indtægter og udgifter, men fører også tilsyn med, at offentlige myndigheder

([103]) Artikel 3 og 5 i lov om revisioner i den offentlige sektor.
([104]) Artikel 7 i lov om revisioner i den offentlige sektor.
([105]) Artikel 8-11 i lov om revisioner i den offentlige sektor.
([106]) Artikel 16 ff. i lov om revisioner i den offentlige sektor.
([107]) Artikel 23, stk. 2, i lov om revisioner i den offentlige sektor.
([108]) Artikel 23, stk. 1, i lov om revisioner i den offentlige sektor.
([109]) Artikel 23, stk. 3, i lov om revisioner i den offentlige sektor.
([110]) Artikel 26 i lov om revisioner i den offentlige sektor.
([111]) Artikel 41 i lov om revisioner i den offentlige sektor.
([112]) Se navnlig afdelingerne under generaldirektøren for revision og inspektion: https://www.police.go.kr/eng/knpa/org/org01.jsp.
([113]) Artikel 24 og 31-35 i lov om revisions- og inspektionsudvalget (»*BAI-loven*«).
([114]) Artikel 2, stk. 1, i BAI-loven.
([115]) Artikel 2, stk. 2, i BAI-loven.
([116]) Artikel 4, stk. 1, i BAI-loven.
([117]) Artikel 5, stk. 1, og artikel 6 i BAI-loven.
([118]) Har f.eks. udøvet hvervet som dommer, offentlig anklager eller advokat i mindst ti år, arbejdet som embedsmand, professor eller i en højere stilling ved et universitet i mindst otte år eller arbejdet i mindst ti år i et børsnoteret selskab eller en statsejet institution (heraf mindst fem år som leder), jf. artikel 7 i BAI-loven.
([119]) Artikel 8 i BAI-loven.
([120]) Artikel 9 i BAI-loven.
([121]) Jf. f.eks. artikel 27 i BAI-loven.

og offentligt ansatte generelt overholder deres forpligtelser, for at forbedre den offentlige forvaltnings funktion ([122]). Udvalgets tilsyn rækker derfor ud over de budgetmæssige aspekter og omfatter også legalitetskontrol.

2.3.3. *Nationalforsamlingen*

Nationalforsamlingen kan undersøge og inspicere offentlige myndigheder ([123]). I forbindelse med en undersøgelse eller inspektion kan nationalforsamlingen anmode om fremlæggelse af dokumenter og pålægge vidner at give møde ([124]). Enhver, der afgiver falsk forklaring i forbindelse med en undersøgelse i nationalforsamlingen, kan idømmes strafferetlige sanktioner (fængsel i op til ti år) ([125]). Processen og resultaterne af inspektioner kan offentliggøres ([126]). Hvis nationalforsamlingen konkluderer, at der har fundet ulovlige eller uretmæssige aktiviteter sted, kan den anmode den relevante offentlige myndighed om at træffe korrigerende foranstaltninger, herunder tilkende erstatning, iværksætte disciplinære foranstaltninger og forbedre sine interne procedurer ([127]). Efter en sådan anmodning skal myndigheden handle straks og aflægge rapport om resultatet til nationalforsamlingen ([128]).

2.3.4. *Kommissionen for beskyttelse af personoplysninger*

Kommissionen for beskyttelse af personoplysninger (»*PIPC*« eller »beskyttelseskommissionen«) fører tilsyn med de strafferetlige håndhævelsesmyndigheders behandling af personoplysninger i overensstemmelse med PIPA. I henhold til artikel 7-8, stk. 3 og 4, og artikel 7-9, stk. 5, i PIPA omfatter PIPC's tilsyn desuden mulige overtrædelser af reglerne om begrænsninger og garantier for indsamling af personoplysninger, herunder reglerne i de specifikke love om indsamling af (elektronisk) bevismateriale med henblik på strafferetlig håndhævelse (jf. afsnit 2.2). I betragtning af kravene i artikel 3, stk. 1, i PIPA vedrørende lovlig og rimelig indsamling af personoplysninger udgør en sådan overtrædelse også en overtrædelse af PIPA, der giver PIPC mulighed for at foretage en undersøgelse og træffe korrigerende foranstaltninger ([129]).

PIPC har under udøvelsen af sin tilsynsfunktion adgang til alle relevante oplysninger ([130]). PIPC kan fremsætte henstillinger til de retshåndhævende myndigheder om, hvordan beskyttelsen af personoplysninger i forbindelse med deres behandlingsaktiviteter kan forbedres, pålægge korrigerende foranstaltninger (f.eks. suspendere databehandlingen eller træffe de nødvendige foranstaltninger til at beskytte personoplysninger) eller henstille, at myndigheden træffer disciplinære foranstaltninger ([131]). Endelig er der fastsat strafferetlige sanktioner for visse PIPA-overtrædelser såsom ulovlig anvendelse eller videregivelse af personoplysninger til tredjemand eller ulovlig behandling af følsomme oplysninger ([132]). I denne forbindelse kan PIPC henvise sagen til den kompetente efterforskningsmyndighed (herunder en anklager) ([133]).

2.3.5. *Den nationale menneskerettighedskommission*

Den nationale menneskerettighedskommission (NHRC) — et uafhængigt organ, der har til opgave at beskytte og fremme grundlæggende rettigheder ([134]) — har beføjelse til at undersøge og afhjælpe overtrædelser af forfatningens artikel 10-22, som omfatter retten til privatlivets fred og privatlivets fred i forbindelse med korrespondance. NHRC består af 11 kommissærer, der udnævnes efter indstilling fra nationalforsamlingen (4), præsidenten (4) og højesteretspræsidenten (3) ([135]). For at blive udnævnt skal en kommissær 1) have været ansat ved et universitet eller et godkendt forskningsinstitut i mindst ti år, som minimum på lektorniveau, 2) have udøvet hvervet som dommer, anklager eller advokat i mindst ti år, 3) have været involveret i menneskerettighedsaktiviteter i mindst ti år (f.eks. for en nonprofitorganisation, ikkestatslig organisation eller international organisation) eller 4) være blevet anbefalet af civilsamfundsgrupper ([136]). Formanden udnævnes af præsidenten blandt kommissærerne, og udnævnelsen skal

([122]) Artikel 20 og 24 i BAI-loven.
([123]) Artikel 128 i lov om nationalforsamlingen og artikel 2, 3 og 15 i lov om inspektion og undersøgelse af statsforvaltningen. Dette omfatter årlige inspektioner af regeringsanliggender som helhed og undersøgelser af specifikke spørgsmål.
([124]) Artikel 10, stk. 1, i lov om inspektion og undersøgelse af statsforvaltningen. Se også artikel 128 og 129 i lov om nationalforsamlingen.
([125]) Artikel 14 lov om vidneudsagn, bedømmelse mv. for nationalforsamlingen.
([126]) Artikel 12-2 i lov om inspektion og undersøgelse af statsforvaltningen.
([127]) Artikel 16, stk. 2, i lov om inspektion og undersøgelse af statsforvaltningen.
([128]) Artikel 16, stk. 3, i lov om inspektion og undersøgelse af statsforvaltningen.
([129]) Jf. PIPC-meddelelse nr. 2021-1 om supplerende regler for fortolkning og anvendelse af lov om beskyttelse af personoplysninger.
([130]) Artikel 63 i PIPA.
([131]) Artikel 61, stk. 2, artikel 65, stk. 1, artikel 65, stk. 2, og artikel 64, stk. 4.
([132]) Artikel 70-74 i PIPA.
([133]) Artikel 65, stk. 1, i PIPA.
([134]) Artikel 1 i lov om menneskerettighedskommissionen (»*NHRC-loven*«).
([135]) Artikel 5, stk. 1 og 2, i NHRC-loven.
([136]) Artikel 5, stk. 3, i NHRC-loven.

bekræftes af nationalforsamlingen ([137]). Kommissærer (herunder formanden) udnævnes for en periode på tre år, der kan forlænges, og kan kun afsættes, hvis de idømmes fængselsstraf eller ikke længere er i stand til at varetage deres opgaver på grund af langvarig psykisk eller fysisk sygdom (i så fald skal to tredjedele af kommissærerne være enige i afsættelsen) ([138]). NHRC-kommissærer må ikke bestride et sideløbende hverv i nationalforsamlingen, lokalråd eller en statslig eller lokal myndighed (som offentligt ansat) ([139]).

NHRC kan indlede en undersøgelse på eget initiativ eller på grundlag af en klage fra en enkeltperson. Som led i sin undersøgelse kan NHRC anmode om fremlæggelse af relevant materiale, foretage inspektioner og indkalde enkeltpersoner til at afgive vidneforklaring ([140]). Efter en undersøgelse kan NHRC udstede henstillinger om at forbedre eller korrigere specifikke politikker og praksis og offentliggøre henstillingerne ([141]). Offentlige myndigheder skal underrette NHRC om deres planer for gennemførelse af disse henstillinger senest 90 dage efter modtagelsen af henstillingerne ([142]). Hvis henstillingerne ikke efterkommes, skal den pågældende myndighed desuden underrette kommissionen herom ([143]). NHRC kan derefter underrette nationalforsamlingen om denne undladelse og/eller offentliggøre den. De offentlige myndigheder efterkommer generelt NHRC's henstillinger og har et stærkt incitament hertil, da deres gennemførelse er blevet vurderet som led i en generel evaluering, som kontoret for samordning af regeringens politikker har foretaget under tilsyn af premierministerens kontor.

2.4. **Individuel klage- og prøvelsesadgang**

2.4.1. *Prøvelsesmekanismer i henhold til PIPA*

Enkeltpersoner kan udøve deres ret i henhold til PIPA til indsigt i og berigtigelse, sletning og suspension behandlingen af personoplysninger, der behandles af strafferetlige håndhævelsesmyndigheder. Der kan anmodes om adgang direkte fra den relevante myndighed eller indirekte via PIPC ([144]). Den kompetente myndighed kan kun begrænse eller nægte adgang, hvis dette er fastsat ved lov, hvis den sandsynligvis vil skade tredjemands liv eller legeme eller er en uberettiget krænkelse af en anden persons ejendom og andre interesser (dvs. hvis den anden persons interesser vejer tungere end den anmodende parts interesser) ([145]). Hvis anmodningen om adgang ikke imødekommes, skal den pågældende oplyses om årsagerne hertil og om, hvordan afgørelsen kan påklages ([146]). En anmodning om berigtigelse eller sletning kan ligeledes afslås, hvis dette er fastsat i anden lovgivning, og i så fald skal den pågældende oplyses om de bagvedliggende årsager og muligheden for at klage ([147]).

Med hensyn til klageadgang kan enkeltpersoner indgive en klage til PIPC, herunder via callcentret for privatlivsbeskyttelse, der drives af Koreas internet- og sikkerhedsagentur ([148]). Desuden kan enkeltpersoner få adgang til mægling gennem udvalget for bilæggelse af tvister om personoplysninger ([149]). Disse prøvelsesmekanismer er tilgængelige både i tilfælde af mulige overtrædelser af reglerne i specifikke love, der fastsætter begrænsninger og garantier for indsamling af personoplysninger (afsnit 2.2), og i PIPA. Desuden kan enkeltpersoner anfægte PIPC's afgørelser eller manglende handling i henhold til lov om forvaltningssager (jf. afsnit 2.4.3).

([137]) Artikel 5, stk. 5, i NHRC-loven.
([138]) Artikel 7, stk. 1, og artikel 8 i NHRC-loven.
([139]) Artikel 10 i NHRC-loven.
([140]) Artikel 36 i NHRC-loven. I henhold til lovens artikel 36, stk. 7, er det muligt at afvise at fremlægge materiale eller genstande, hvis det vil krænke den fortrolige karakter af statslige forhold, der kan have væsentlig indvirkning på statens sikkerhed eller diplomatiske forbindelser eller vil udgøre en alvorlig hindring for en strafferetlig efterforskning eller verserende retssag. I sådanne tilfælde kan kommissionen anmode lederen af det relevante organ (som skal overholde reglerne i god tro) om yderligere oplysninger, hvis det er nødvendigt for at undersøge, om afvisningen af at fremlægge oplysningerne er berettiget.
([141]) Artikel 25, stk. 1, i NHRC-loven.
([142]) Artikel 25, stk. 3, i NHRC-loven.
([143]) Artikel 25, stk. 4, i NHRC-loven.
([144]) Artikel 35, stk. 2, i PIPA.
([145]) Artikel 35, stk. 4, i PIPA.
([146]) Artikel 42, stk. 2, i PIPA-gennemførelsesdekretet.
([147]) Artikel 36, stk. 1-2, i PIPA og artikel 43, stk. 3, i PIPA-gennemførelsesdekretet.
([148]) Artikel 62 i PIPA.
([149]) Artikel 40-50 i PIPA og artikel 48-2 til 57 i PIPA-gennemførelsesdekretet.

2.4.2. *Klageadgang ved den nationale menneskerettighedskommission*

NHRC behandler klager fra enkeltpersoner (både koreanske og udenlandske statsborgere) vedrørende menneskerettighedskrænkelser begået af offentlige myndigheder ([150]). Der er intet krav om søgsmålskompetence for personer, der ønsker at indgive en klage til NHRC ([151]). Som følge heraf behandler NHRC klagen, selv om den pågældende person ikke kan påvise en faktisk skade på tidspunktet for antagelsen. I forbindelse med indsamling af personoplysninger med henblik på strafferetlig håndhævelse vil en person derfor ikke være forpligtet til at påvise, at de koreanske offentlige myndigheder rent faktisk har fået adgang til vedkommendes personoplysninger, inden klagen kan antages til behandling ved NHRC. En person kan også anmode om at få afgjort klagesagen gennem mægling ([152]).

I forbindelse med undersøgelsen af en klage kan NHRC gøre brug af sine undersøgelsesbeføjelser, herunder ved at anmode om forelæggelse af relevant materiale, foretage inspektioner og indkalde enkeltpersoner til at afgive vidneforklaring ([153]). Hvis undersøgelsen viser, at der er sket en overtrædelse af relevante love, kan NHRC fremsætte henstillinger om gennemførelse af foranstaltninger eller ændring eller forbedring af enhver relevant lov, institution, politik eller praksis ([154]). De foreslåede foranstaltninger kan omfatte mægling, ophør af krænkelsen af menneskerettighederne, skadeserstatning og foranstaltninger til at forhindre, at de samme eller lignende krænkelser gentager sig ([155]). I tilfælde af ulovlig indsamling af personoplysninger i henhold til gældende regler kan afhjælpende foranstaltninger omfatte sletning af de indsamlede personoplysninger. NHRC kan vedtage hasteforanstaltninger, hvis der anses for at være stor sandsynlighed for, at en overtrædelse fortsætter, og det anses for sandsynligt, at der vil opstå skade, som er vanskelig at afhjælpe, hvis der ikke gribes ind ([156]).

NHRC har ikke beføjelse til at træffe bindende afgørelser, men NHRC's afgørelser (f.eks. en afgørelse om ikke at fortsætte undersøgelsen af en klage) ([157]) og henstillinger kan indbringes for de koreanske domstole i henhold til lov om forvaltningssager (jf. afsnit 2.4.3 nedenfor) ([158]). Hvis NHRC's konklusioner viser, at personoplysninger er indsamlet ulovligt af en offentlig myndighed, kan en person desuden anlægge en sag ved de koreanske domstole mod denne offentlige myndighed, f.eks. ved at anfægte indsamlingen i henhold til lov om forvaltningssager, indgive en forfatningsretlig klage i henhold til lov om forfatningsdomstolen eller kræve skadeserstatning efter lov om erstatning fra staten (jf. afsnit 2.4.3 nedenfor).

2.4.3. *Retslig prøvelse*

Enkeltpersoner kan påberåbe sig de begrænsninger og garantier, der er beskrevet i de foregående afsnit, ved at indbringe en sag for de koreanske domstole via forskellige mekanismer.

For det første kan den berørte person og dennes advokat i overensstemmelse med CPA være til stede på tidspunktet for fuldbyrdelse af en kendelse om ransagning eller beslaglæggelse, og de kan derfor gøre indsigelse på tidspunktet for fuldbyrdelse af kendelsen ([159]). Desuden indeholder CPA en såkaldt »kvasiklagemekanisme«, som giver enkeltpersoner mulighed for at anmode den kompetente ret om at annullere eller ændre en disposition truffet af en anklager eller politiet vedrørende en beslaglæggelse ([160]). Dette giver enkeltpersoner mulighed for at anfægte de foranstaltninger, der er truffet for at fuldbyrde en retskendelse om beslaglæggelse.

([150]) Udtrykket »bosiddende« skal ses i sammenhæng med begrebet »jurisdiktion« og ikke »område«, selv om der i artikel 4 i NHRC-loven henvises til statsborgere og udlændinge, der er bosiddende i Republikken Korea. Hvis en udlændings grundlæggende rettigheder krænkes af nationale institutioner i Korea, kan den pågældende derfor indgive en klage til NHRC. Se f.eks. det tilsvarende spørgsmål på NHRC's websted med ofte stillede spørgsmål, som findes på https://www.humanrights.go.kr/site/program/board/basicboard/list?boardtypeid=7025&menuid=002004005001&pagesize=10&currentpage=2. Dette ville være tilfældet, hvis de koreanske offentlige myndigheder ulovligt tilgår personoplysninger om en udlænding, der er overført til Korea.

([151]) En klage skal i princippet indgives inden for et år efter krænkelsen, men NHRC kan stadig beslutte at undersøge en klage, der indgives efter denne frist, så længe forældelsesfristen i henhold til straffe- eller civilretten ikke er udløbet (artikel 32, stk. 1, nr. 4, i NHRC-loven).

([152]) Artikel 42 ff. i NHRC-loven.

([153]) Artikel 36 og 37 i NHRC-loven.

([154]) Artikel 44 i NHRC-loven.

([155]) Artikel 42, stk. 4, i NHRC-loven.

([156]) Artikel 48 i NHRC-loven.

([157]) Hvis NHRC f.eks. undtagelsesvis ikke har mulighed for at inspicere visse materialer eller faciliteter, fordi de vedrører statshemmeligheder, der kan have en væsentlig indvirkning på statens sikkerhed eller diplomatiske forbindelser, eller hvis inspektionen vil udgøre en alvorlig hindring for en strafferetlig efterforskning eller verserende retssag (jf. fodnote 166), og hvis dette forhindrer NHRC i at foretage den nødvendige undersøgelse for at vurdere, om den modtagne klage er begrundet, underretter udvalget den pågældende om begrundelsen for, at klagen blev afvist, i overensstemmelse med artikel 39 i NHRC-loven. I dette tilfælde kan den pågældende anfægte NHRC's afgørelse i henhold til lov om forvaltningssager.

([158]) Jf. f.eks. Seoul High Courts afgørelse 2007NU27259 af 18. april 2008, stadfæstet ved højesterets afgørelse nr. 2008Du7854 af 9. oktober 2008, Seoul High Courts afgørelse nr. 2017Nu69382 af 2. februar 2018.

([159]) Artikel 121 og 219 i CPA.

([160]) Artikel 417 i CPA sammenholdt med artikel 414, stk. 2, i CPA. Se også højesterets afgørelse nr. 97Mo66 af 29. september 1997.

Enkeltpersoner kan desuden opnå skadeserstatning ved de koreanske domstole. I henhold til lov om erstatning fra staten kan personer søge erstatning for skade, som offentligt ansatte har forvoldt under udøvelsen af deres officielle hverv i strid med loven ([161]). Et krav i henhold til lov om erstatning fra staten kan indgives til et specialiseret »erstatningsråd« eller direkte til de koreanske domstole ([162]). Hvis offeret er udenlandsk statsborger, finder lov om erstatning fra staten anvendelse, hvis vedkommendes hjemland ligeledes sikrer koreanske statsborgere erstatning fra staten ([163]). I henhold til retspraksis er denne betingelse opfyldt, hvis kravene vedrørende anmodning om erstatning i det andet land »*ikke i væsentlig grad udlignes mellem Korea og det andet land*« og »*generelt ikke er strengere end de krav, der er fastsat i Korea, og der ikke er nogen materiel forskel*« ([164]). Civilloven regulerer statens erstatningsansvar, og som følge heraf omfatter statens erstatningsansvar også immateriel skade (f.eks. psykiske lidelser) ([165]).

Der er et yderligere retsmiddel i PIPA i forbindelse med overtrædelser af databeskyttelsesreglerne. I henhold til artikel 39 i PIPA kan enhver, der lider skade som følge af en overtrædelse af PIPA eller tab, tyveri, videregivelse, forfalskning, ændring af eller skade på sine personoplysninger, få erstatning ved domstolene. Der er ikke noget tilsvarende krav om gensidighed som i lov om erstatning fra staten.

Ud over skadeserstatning er der adgang til administrativ prøvelse i forbindelse med forvaltningsorganers handlinger eller undladelser i henhold til lov om forvaltningssager. Enhver kan anfægte en disposition (dvs. udøvelse af eller afvisning af at udøve offentlig myndighed i en bestemt sag) eller undladelse (et forvaltningsorgans langvarige undladelse af at træffe en bestemt disposition i strid med en retlig forpligtelse hertil), hvilket kan føre til tilbagekaldelse/ændring af en ulovlig disposition, udstedelse af en afgørelse om ugyldighed (dvs. en afgørelse om, at dispositionen ikke har retsvirkning eller ikke eksisterer i retsordenen) eller udstedelse af en afgørelse om, at en undladelse er ulovlig ([166]). For at kunne anfægte en administrativ disposition skal den have direkte indvirkning på borgerlige rettigheder og pligter ([167]). Dette omfatter foranstaltninger til indsamling af personoplysninger, enten direkte (f.eks. aflytning af kommunikation) eller gennem en anmodning om videregivelse (f.eks. til en tjenesteudbyder).

Ovennævnte klager kan i første omgang indbringes for administrative klageudvalg, der er nedsat under visse offentlige myndigheder (f.eks. NIS og NHRC), eller for det centrale administrative klageudvalg, der er nedsat under kommissionen for korruptionsbekæmpelse og borgerlige rettigheder ([168]). En sådan administrativ klage er en alternativ og mere uformel mulighed for at anfægte en offentlig myndigheds disposition eller undladelse. Der kan dog også indbringes en sag direkte for de koreanske domstole i henhold til lov om forvaltningssager.

En anmodning om tilbagekaldelse/ændring af en disposition i henhold til lov om forvaltningssager kan indgives af enhver, der har en retlig interesse i at anmode om tilbagekaldelsen/ændringen eller blive genindsat i sine rettigheder ved tilbagekaldelsen/ændringen, hvis dispositionen ikke længere har virkning ([169]). På samme måde kan en person, der har en retlig interesse heri, anlægge en sag for at få fastslået, at en disposition er ugyldig, hvorimod en sag for at få fastslået, at en undladelse er ulovlig, kan anlægges af enhver, der har fremsat en anmodning om en disposition og har en retlig interesse i at få fastslået, at en undladelse er ulovlig ([170]). Ifølge højesterets retspraksis fortolkes »retlig interesse« som en »retligt beskyttet interesse«, dvs. en direkte og specifik interesse, der er beskyttet af love og administrative bestemmelser, som administrative dispositioner er baseret på (dvs. ikke offentlighedens generelle, indirekte og abstrakte interesser) ([171]). Enkeltpersoner har derfor en retlig interesse i tilfælde af overtrædelse af begrænsningerne og garantierne for indsamling af deres personoplysninger med henblik på strafferetlig håndhævelse (i henhold til specifik lovgivning eller PIPA). En endelig dom i henhold til lov om forvaltningssager er bindende for parterne ([172]).

En anmodning om tilbagekaldelse/ændring af en disposition og en anmodning om at få fastslået, at en undladelse er ulovlig, indgives senest 90 dage efter den dato, hvor personen får kendskab til dispositionen/undladelsen, og i

([161]) Artikel 2, stk. 1, i lov om erstatning fra staten.
([162]) Artikel 9 og 12 i lov om erstatning fra staten. Ved loven oprettes distriktsråd (under forsæde af vicestatsadvokaten ved den tilsvarende anklagemyndighed), et centralråd (under forsæde af vicejustitsministeren) og et særligt råd (under forsæde af viceforsvarsministeren med ansvar for erstatningskrav for skade forvoldt af militærpersonel eller civilansatte i militæret). Erstatningskrav behandles i princippet af distriktsråd, som under visse omstændigheder skal videresende sagerne til det centrale/særlige råd, f. eks. hvis erstatningen overstiger et vist beløb, eller hvis en person anmoder om fornyet behandling. Alle råd består af medlemmer udpeget af justitsministeren (f.eks. blandt embedsmænd i justitsministeriet, retsembedsmænd, advokater og personer med ekspertise inden for erstatning fra staten) og er underlagt specifikke regler om interessekonflikter (jf. artikel 7 i gennemførelsesdekretet til lov om erstatning fra staten).
([163]) Artikel 7 i lov om erstatning fra staten.
([164]) Højesterets afgørelse nr. 2013Da208388 af 11. juni 2015.
([165]) Jf. artikel 8 i lov om erstatning fra staten og artikel 751 i civilloven.
([166]) Artikel 2 og 4 i lov om forvaltningssager.
([167]) Højesterets afgørelse 98Du18435 af 22. oktober 1999, højesterets afgørelse 99Du1113 af 8. september 2000 og højesterets afgørelse 2010Du3541 af 27. september 2012.
([168]) Artikel 6 i lov om administrative klager og artikel 18, stk. 1, i lov om forvaltningssager.
([169]) Artikel 12 i lov om forvaltningssager.
([170]) Artikel 35 og 36 i lov om forvaltningssager.
([171]) Højesterets afgørelse nr. 2006Du330 af 26. marts 2006.
([172]) Artikel 30, stk. 1, i lov om forvaltningssager.

princippet senest et år efter datoen, hvor dispositionen blev truffet, eller datoen for undladelsen, medmindre der er berettigede grunde hertil ([173]). I henhold til højesterets retspraksis skal begrebet »berettigede grunde« fortolkes bredt og kræver en vurdering af, om det er samfundsmæssigt acceptabelt at give mulighed for at indbringe en forsinket klage i lyset af alle sagens omstændigheder ([174]). Dette omfatter f.eks. (men er ikke begrænset til) årsager til forsinkelser, som den pågældende part ikke kan holdes ansvarlig for (dvs. situationer, der ligger uden for klagers kontrol, f.eks. hvis vedkommende ikke er blevet underrettet om indsamlingen af sine personoplysninger) eller force majeure (f.eks. naturkatastrofe eller krig).

Endelig kan enkeltpersoner også indgive en forfatningsmæssig klage til forfatningsdomstolen ([175]). På grundlag af lov om forfatningsdomstolen kan enhver, hvis grundlæggende forfatningssikrede rettigheder krænkes som følge af udøvelsen eller den manglende udøvelse af offentlig myndighed (bortset fra domstolsafgørelser), indgive en forfatningsmæssig klage. Hvis der findes andre retsmidler, skal disse først udtømmes. I henhold til forfatningsdomstolens retspraksis kan udenlandske statsborgere indgive en forfatningsmæssig klage, i det omfang deres grundlæggende rettigheder er anerkendt i den koreanske forfatning (se forklaringerne i afsnit 1.1) ([176]). Forfatningsmæssige klager skal indgives senest 90 dage efter, at den pågældende har fået kendskab til overtrædelsen, og senest et år efter, at den er begået. En klage vil stadig kunne antages til realitetsbehandling, hvis der foreligger »berettigede grunde« som fortolket i overensstemmelse med højesterets retspraksis beskrevet ovenfor, da proceduren i lov om forvaltningssager finder anvendelse på tvister i henhold til lov om forfatningsdomstolen ([177]).

Hvis andre retsmidler først skal udtømmes, skal der indgives en forfatningsmæssig klage senest 30 dage efter den endelige afgørelse om et sådant retsmiddel ([178]). Forfatningsdomstolen kan ugyldiggøre den udøvelse af offentlig myndighed, der forårsagede overtrædelsen, eller fastslå, at en bestemt undladelse af at handle er forfatningsstridig ([179]). I så fald er den relevante myndighed forpligtet til at træffe foranstaltninger for at efterkomme domstolens afgørelse.

3. MYNDIGHEDSADGANG AF HENSYN TIL DEN NATIONALE SIKKERHED

3.1. Kompetente offentlige myndigheder på området national sikkerhed

Republikken Korea har to særlige efterretningsagenturer, nemlig NIS og forsvarssikkerhedskommandoen. Derudover kan politiet og anklagemyndigheden også indsamle personoplysninger til nationale sikkerhedsformål.

NIS er oprettet ved lov om den nationale efterretningstjeneste (»*NIS-loven*«) og er direkte underlagt præsidentens kontrol og tilsyn ([180]). NIS indsamler, kompilerer og formidler navnlig oplysninger om andre lande (herunder Nordkorea) ([181]), efterretninger forbindelse med bekæmpelse af spionage (herunder militær og industriel spionage), terrorisme og internationale kriminelle syndikaters aktiviteter, efterretninger om visse former for kriminalitet rettet mod den offentlige og nationale sikkerhed (f.eks. indenlandsk oprør, aggression udefra) og efterretninger i forbindelse med opgaven med at garantere internetsikkerheden og forebygge eller bekæmpe cyberangreb og -trusler ([182]). I NIS-loven, hvorved NIS blev oprettet, fastlægges efterretningstjenestens opgaver og de generelle principper, der danner grundlag for alle dens aktiviteter. NIS skal som et generelt princip være politisk neutral og beskytte den enkeltes friheder og rettigheder ([183]). Chefen for NIS har til opgave at udarbejde generelle retningslinjer, der fastsætter principperne, anvendelsesområdet og procedurerne for udførelse af efterretningstjenestens opgaver i forbindelse med indsamling og anvendelse af oplysninger, og skal forelægge dem for nationalforsamlingen ([184]). Nationalforsamlingen kan (gennem sit efterretningsudvalg) kræve, at retningslinjerne korrigeres eller suppleres, hvis den mener, at de er ulovlige eller uhensigtsmæssige. Chefen for NIS og medarbejderne må mere generelt ikke misbruge deres offentlige myndighedsbeføjelser under udførelsen af deres opgaver til at tvinge nogen institution, organisation eller enkeltperson til at gøre noget, som de ikke er forpligtet til, eller hindre en person i at udøve sine rettigheder ([185]). Desuden skal enhver form for censur af post, aflytning af telekommunikation, indsamling af lokaliseringsdata, indsamling af kommunikationsbekræftelsesdata eller NIS' optagelse af eller lytning

([173]) Artikel 20 i lov om forvaltningssager. Denne frist gælder også for en anmodning om at få fastslået, at en undladelse er ulovlig, jf. artikel 38, stk. 2, i lov om forvaltningsretssager.
([174]) Højesterets afgørelse 90Nu6521 af 28. juni 1991.
([175]) Artikel 68, stk. 1, i lov om forfatningsdomstolen.
([176]) Forfatningsdomstolens afgørelse nr. 99HeonMa194 af 29. november 2001.
([177]) Artikel 40 i lov om forfatningsdomstolen.
([178]) Artikel 69 i lov om forfatningsdomstolen.
([179]) Artikel 75, stk. 3, i lov om forfatningsdomstolen.
([180]) Artikel 2 og artikel 4, stk. 2, i NIS-loven.
([181]) Dette begreb omfatter ikke oplysninger om enkeltpersoner, men generelle oplysninger om andre lande (tendenser, udvikling) og om aktiviteter, der udføres af statslige aktører i tredjelande.
([182]) Artikel 3, stk. 1, i NIS-loven
([183]) Artikel 3, stk. 1, artikel 6, stk. 2, artikel 11 og 21. Se også reglerne om interessekonflikter, navnlig artikel 10 og 12.
([184]) Artikel 4, stk. 2, i NIS-loven
([185]) Artikel 13 i NIS-loven.

til privat kommunikation være i overensstemmelse med CPPA, lov om lokaliseringsdata eller CPA ([186]). Ethvert misbrug af beføjelser eller indsamling af oplysninger i strid med disse love er omfattet af strafferetlige sanktioner ([187]).

Forsvarssikkerhedskommandoen er et militært efterretningsagentur oprettet under forsvarsministeriet. Den har ansvaret for militære sikkerhedsspørgsmål, militære strafferetlige efterforskninger (omfattet af lov om militærdomstolen) og militære efterretninger. Generelt overvåger forsvarssikkerhedskommandoen ikke civile, medmindre dette er nødvendigt for at varetage kommandoens militære funktioner. Der kan foretages efterforskning vedrørende militærpersonel, civilansatte i militæret, personer under militær uddannelse, personer i militærreserven eller rekruttjeneste og krigsfanger ([188]). Når forsvarssikkerhedskommandoen indsamler kommunikationsdata til nationale sikkerhedsformål, er den underlagt de begrænsninger og garantier, der er fastsat i CPPA og gennemførelsesdekretet hertil.

3.2. **Retsgrundlag og begrænsninger**

CPPA, lov om bekæmpelse af terrorisme og beskyttelse af borgerne og den offentlige sikkerhed (»*antiterrorloven*«) og TBA udgør retsgrundlaget for indsamling af personoplysninger til nationale sikkerhedsformål og fastsætter de gældende begrænsninger og garantier ([189]). Disse begrænsninger og garantier som beskrevet i de næste afsnit sikrer, at indsamlingen og behandlingen af oplysninger begrænses til, hvad der er strengt nødvendigt for at nå et legitimt mål. Dette udelukker massiv og vilkårlig indsamling af personoplysninger til nationale sikkerhedsformål.

3.2.1. *Indsamling af kommunikationsdata*

3.2.1.1. Efterretningsagenturers indsamling af kommunikationsdata

3.2.1.1.1. Retsgrundlag

CPPA giver efterretningsagenturer beføjelse til at indsamle kommunikationsdata og pålægger kommunikationsudbydere at samarbejde om anmodninger fra disse agenturer ([190]). Som beskrevet i afsnit 2.2.2.1 skelner CPPA mellem indsamling af indholdet af kommunikation (dvs. »*kommunikationsbegrænsende foranstaltninger*« såsom »*aflytning*« eller »*censur*« ([191])) og indsamling af »*kommunikationsbekræftelsesdata*« ([192]).

Tærsklen for indsamling af disse to typer oplysninger varierer, men de gældende procedurer og garantier er i vid udstrækning identiske ([193]). Indsamlingen af kommunikationsbekræftelsesdata (eller metadata) kan finde sted for at forebygge trusler mod den nationale sikkerhed ([194]). Der gælder en højere tærskel for gennemførelse af kommunikationsbegrænsende foranstaltninger (dvs. indsamling af indholdet af kommunikation), som kun kan træffes, når den nationale sikkerhed forventes at blive bragt i alvorlig fare, og indsamlingen af efterretninger er nødvendig for at forebygge en sådan fare (dvs. hvis der er en alvorlig risiko for den nationale sikkerhed, og indsamlingen er nødvendig for at forebygge den) ([195]). Desuden må der kun gives adgang til indholdet af kommunikation som en sidste udvej for at sikre den nationale sikkerhed, og der skal gøres en indsats for at minimere krænkelsen af privatlivets fred i forbindelse med kommunikation ([196]). Selv når den relevante godkendelse/tilladelse er opnået, skal sådanne foranstaltninger straks bringes til ophør, når de ikke længere er nødvendige, hvorved det sikres, at enhver krænkelse af den enkeltes ret til kommunikationshemmelighed begrænses til et minimum ([197]).

3.2.1.1.2. Begrænsninger og garantier for indsamlingen af kommunikationsdata, der som minimum involverer en koreansk statsborger

Indsamling af kommunikationsdata (både indhold og metadata), hvor en af eller begge parter i kommunikationen er koreanske statsborgere, må kun finde sted med tilladelse fra en retspræsident ved High

([186]) Artikel 14 i NIS-loven.
([187]) Artikel 22 og 23 i NIS-loven.
([188]) Artikel 1 i lov om militærdomstole.
([189]) Politiet og NIS efterforsker kriminalitet i forbindelse med den nationale sikkerhed på grundlag af CPA, hvorimod forsvarssikkerhedskommandoen er underlagt lov om militærdomstolen.
([190]) Artikel 15-2 i CPPA.
([191]) Artikel 2, stk. 6 og 7, i CPPA.
([192]) Artikel 2, stk. 11, i CPPA.
([193]) Se også artikel 13-4, stk. 2, i CPPA og artikel 37, stk. 4, i CPPA-gennemførelsesdekretet, hvori det fastsættes, at de procedurer, der gælder for indsamling af indholdet af kommunikation, finder tilsvarende anvendelse på indsamling af kommunikationsbekræftelsesdata.
([194]) Artikel 13-4 i CPPA.
([195]) Artikel 7, stk. 1, i CPPA.
([196]) Artikel 3, stk. 2, i CPPA.
([197]) Artikel 2 i CPPA-gennemførelsesdekretet.

Court ([198]). Anmodningen fra efterretningsagenturet skal indgives skriftligt til en anklager eller en højere anklagemyndighed ([199]). Den skal indeholde oplysninger om grundene til indsamlingen (dvs. at den nationale sikkerhed forventes at blive bragt i alvorlig fare, eller at indsamlingen er nødvendig for at forebygge trusler mod den nationale sikkerhed) og materiale, der underbygger disse grunde og påviser, at der foreligger en prima facie-sag, samt nærmere oplysninger om anmodningen (dvs. om formål, den eller de overvågede personer, omfang, faktisk indsamlingsperiode, og om hvordan og hvor indsamlingen vil finde sted) ([200]). Anklageren/den højere anklagemyndighed anmoder derefter en retspræsident ved High Court om tilladelse ([201]). Retspræsidenten kan kun give skriftlig tilladelse, hvis han/hun mener, at ansøgningen er berettiget, og afviser anmodningen, hvis han/hun anser den for ubegrundet ([202]). I kendelsen angives type, formål, mål, omfang og faktisk indsamlingsperiode, samt hvor og hvordan indsamlingen kan finde sted ([203]).

Der gælder særlige regler, hvis foranstaltningen tager sigte på efterforskning af en sammensværgelse, som truer den nationale sikkerhed, og der foreligger en nødsituation, som gør det umuligt at gennemføre ovennævnte procedurer ([204]). Hvis disse betingelser er opfyldt, kan efterretningsagenturer gennemføre overvågningsforanstaltninger uden en forudgående retskendelse ([205]). Efterretningsagenturerne skal dog umiddelbart efter gennemførelsen af hasteforanstaltningerne anmode om en retskendelse. Indsamlingen skal straks indstilles, hvis retskendelsen ikke opnås senest 36 timer efter iværksættelsen af foranstaltningerne ([206]). Indsamling af oplysninger i nødsituationer skal altid finde sted i overensstemmelse med en »erklæring om censur/aflytning i nødsituationer«, og det efterretningsagentur, der foretager indsamlingen, skal føre et register over alle hasteforanstaltninger ([207]).

Hvis overvågningen afsluttes inden for kort tid og uden en retskendelse, skal chefen for den kompetente højere anklagemyndighed sende en meddelelse om hasteforanstaltninger udarbejdet af efterretningsagenturet til præsidenten for den kompetente ret, som fører registret over hasteforanstaltninger ([208]). Dette gør det muligt for retten at undersøge, om indsamlingen er lovlig.

3.2.1.1.3. Begrænsninger og garantier for indsamlingen af kommunikationsdata, der kun involverer ikkekoreanske statsborgere

Hvis efterretningsagenturerne udelukkende skal indsamle oplysninger om kommunikation mellem ikkekoreanske statsborgere, skal de indhente en skriftlig forhåndsgodkendelse fra præsidenten ([209]). Denne kommunikation kan kun indsamles til nationale sikkerhedsformål, hvis den falder ind under en af de opstillede kategorier, dvs. kommunikation mellem regeringsembedsmænd eller andre enkeltpersoner fra lande, der er fjendtligt indstillet over for Republikken Korea, udenlandske organer, grupper eller statsborgere, der mistænkes for at deltage i antikoreanske aktiviteter ([210]), eller medlemmer af grupper, der opererer på Den Koreanske Halvø, men reelt uden at være underlagt Republikken Koreas suverænitet, og deres paraplygrupper i andre lande ([211]). Hvis den ene part i kommunikationen derimod er en koreansk statsborger og den anden ikkekoreansk statsborger, kræves rettens godkendelse i overensstemmelse med den procedure, der er beskrevet i afsnit 3.2.1.1.2.

Lederen af et efterretningsagentur skal forelægge en plan for de påtænkte foranstaltninger for chefen for NIS ([212]). Chefen for NIS vurderer, om planen er hensigtsmæssig, og forelægger den for præsidenten til godkendelse, hvis dette er tilfældet ([213]). De oplysninger, der skal indgå i planen, er de samme som de oplysninger, der skal indgå i en anmodning om en retskendelse til at indsamle oplysninger om koreanske statsborgere (jf. ovenfor) ([214]). Den skal navnlig indeholde oplysninger om grundene til indsamlingen (dvs. at den nationale sikkerhed forventes at blive bragt i alvorlig fare, eller at indsamlingen er nødvendig for at forebygge trusler mod den nationale sikkerhed), oplysninger om de vigtigste grunde til mistanke og materiale, der underbygger disse grunde og påviser, at der foreligger en prima facie-sag, samt nærmere

([198]) Artikel 7, stk. 1, nr. 1, i CPPA. Den kompetente ret er den High Court, der har kompetence på det sted, hvor den ene eller begge overvågede parter har bopæl eller hjemsted.
([199]) Artikel 7, stk. 3, i CPPA-gennemførelsesdekretet.
([200]) Artikel 7, stk. 3, og artikel 6, stk. 4, i CPPA.
([201]) Artikel 7, stk. 4, i CPPA-gennemførelsesdekretet. I anklagerens anmodning til retten angives de vigtigste grunde til mistanke og, i det omfang der samtidig anmodes om flere tilladelser, begrundelsen herfor (jf. artikel 4 i CPPA-gennemførelsesdekretet).
([202]) Artikel 7, stk. 3, artikel 6, stk. 5, og artikel 6, stk. 9, i CPPA.
([203]) Artikel 7, stk. 3, og artikel 6, stk. 6, i CPPA.
([204]) Artikel 8 i CPPA.
([205]) Artikel 8, stk. 1, i CPPA.
([206]) Artikel 8, stk. 2, i CPPA.
([207]) Artikel 8, stk. 4, i CPPA. Jf. afsnit 2.2.2.2 ovenfor om hasteforanstaltninger i forbindelse med retshåndhævelse.
([208]) Artikel 8, stk. 5 og 7, i CPPA. I denne meddelelse angives formål, mål, omfang, varighed, gennemførelsessted og overvågningsmetode samt begrundelsen for ikke at indgive en anmodning, inden foranstaltningen træffes (artikel 8, stk. 6, i CPPA).
([209]) Artikel 7, stk. 1, nr. 2, i CPPA.
([210]) Herved forstås aktiviteter, der truer landets eksistens og sikkerhed, den demokratiske orden eller folkets overlevelse og frihed.
([211]) Hvis den ene part er en person som beskrevet i artikel 7, stk. 1, nr. 2, i CPPA, og den anden er ukendt eller ikke kan identificeres, finder proceduren i artikel 7, stk. 1, nr. 2, desuden anvendelse.
([212]) Artikel 8, stk. 1, i CPPA-gennemførelsesdekretet. Chefen for NIS udnævnes af præsidenten med parlamentets godkendelse (artikel 7 i NIS-loven).
([213]) Artikel 8, stk. 2, i CPPA-gennemførelsesdekretet.
([214]) Artikel 8, stk. 3, i CPPA-gennemførelsesdekretet sammenholdt med artikel 6, stk. 4, i CPPA.

oplysninger om anmodningen (dvs. om formål, den eller de overvågede personer, omfang, faktisk indsamlingsperiode, og om hvordan og hvor indsamlingen vil finde sted). Hvis der anmodes om flere tilladelser samtidig, angives formål og begrundelse ([215]).

I nødsituationer ([216]) skal der indhentes forudgående godkendelse fra den minister, som det relevante efterretningsagentur er underlagt. I dette tilfælde skal efterretningsagenturet dog anmode om præsidentens godkendelse umiddelbart efter iværksættelsen af hasteforanstaltningerne. Indsamlingen skal straks indstilles, hvis efterretningsagenturet ikke opnår godkendelsen senest 36 timer efter indgivelsen af anmodningen ([217]). I sådanne tilfælde vil de indsamlede oplysninger altid blive tilintetgjort.

3.2.1.1.4. Generelle begrænsninger og garantier

Efterretningsagenturer, der anmoder private enheder om at samarbejde, skal indhente en retskendelse eller en tilladelse fra præsidenten eller en kopi af forsiden af en erklæring om censur i nødsituationer, som de skal give til den pågældende enhed, der skal opbevare den ([218]). Enheder, der anmodes om at videregive oplysninger til efterretningsagenturer på grundlag af CPPA, kan nægte at gøre dette, hvis der i kendelsen/tilladelsen eller erklæringen om censur i nødsituationer angives en forkert identifikator (f.eks. et telefonnummer tilhørende en anden person end den identificerede person). Desuden må adgangskoder, der anvendes til kommunikation, under alle omstændigheder ikke videregives ([219]).

Efterretningsagenturer kan overdrage gennemførelsen af kommunikationsbegrænsende foranstaltninger eller indsamling af kommunikationsbekræftelsesdata til et postkontor eller en teleudbyder (som defineret i telekommunikationsloven) ([220]). Både det pågældende efterretningsagentur og den udbyder, der modtager en anmodning om samarbejde, skal opbevare fortegnelser over formålet med anmodningen om foranstaltninger, datoen for gennemførelsen eller samarbejdet og genstanden for foranstaltningerne (f.eks. post, telefon, e-mail) i tre år ([221]). Teleudbydere, der videregiver kommunikationsbekræftelsesdata, skal opbevare oplysninger om indsamlingshyppigheden i syv år og aflægge rapport til ministeren for videnskab og IKT to gange om året ([222]).

Efterretningsagenturer skal aflægge rapport om de oplysninger, de har indsamlet, og om resultaterne af overvågningen til chefen for NIS ([223]). Med hensyn til indsamlingen af kommunikationsbekræftelsesdata skal der føres fortegnelser over, at der er indgivet en anmodning om sådanne oplysninger, og over selve den skriftlige anmodning og den institution, der har indgivet den ([224]).

Både kommunikationsindhold og kommunikationsbekræftelsesdata kan højst indsamles i fire måneder, og indsamlingen skal straks bringes til ophør, hvis det forfulgte mål nås tidligere ([225]). Hvis betingelserne for tilladelsen fortsat er opfyldt, kan fristen forlænges med op til fire måneder med rettens tilladelse eller præsidentens godkendelse. Anmodningen om godkendelse til at forlænge overvågningsforanstaltningerne skal indgives skriftligt med angivelse af begrundelsen for anmodningen om forlængelse, og der skal vedlægges dokumentation ([226]).

Afhængigt af retsgrundlaget for indsamlingen underrettes enkeltpersoner generelt, når deres kommunikation indsamles. Lederen af efterretningsagenturet skal navnlig, uanset om de indsamlede oplysninger vedrører indholdet af kommunikation eller kommunikationsbekræftelsesdata, og uanset om oplysningerne er indhentet efter den almindelige procedure eller hasteproceduren, skriftligt underrette den pågældende om overvågningsforanstaltningen senest 30 dage efter den dato, hvor overvågningen ophørte ([227]). Underretningen skal indeholde 1) en angivelse af, at oplysningerne er indsamlet, 2) gennemførelsesmyndigheden og 3) gennemførelsesperioden. Hvis underretningen sandsynligvis vil bringe

([215]) Artikel 8, stk. 3, og artikel 4 i CPPA-gennemførelsesdekretet.
([216]) Hvis foranstaltningen er rettet mod en sammensværgelse, der truer den nationale sikkerhed, og der ikke er tilstrækkelig tid til at indhente præsidentens godkendelse og manglende vedtagelse af hasteforanstaltninger kan være til skade for den nationale sikkerhed (artikel 8, stk. 8, i CPPA).
([217]) Artikel 8, stk. 9, i CPPA.
([218]) Artikel 9, stk. 2, i CPPA og artikel 12 i CPPA-gennemførelsesdekretet.
([219]) Artikel 9, stk. 4, i CPPA.
([220]) Artikel 13 i CPPA-gennemførelsesdekretet.
([221]) Artikel 9, stk. 3, i CPPA og artikel 17, stk. 2, i CPPA-gennemførelsesdekretet. Denne frist gælder ikke for kommunikationsbekræftelsesdata (jf. artikel 39 i CPPA-gennemførelsesdekretet).
([222]) Artikel 13, stk. 7, i CPPA og artikel 39 i CPPA-gennemførelsesdekretet.
([223]) Artikel 18, stk. 3, i CPPA-gennemførelsesdekretet.
([224]) Artikel 13, stk. 5, og artikel 13-4, stk. 3, i CPPA.
([225]) Artikel 7, stk. 2, i CPPA.
([226]) Artikel 7, stk. 2, i CPPA og artikel 5 i CPPA-gennemførelsesdekretet.
([227]) Artikel 9-2, stk. 3, i CPPA. I overensstemmelse med artikel 13-4 i CPPA gælder dette både for indsamling af indholdet af kommunikation og kommunikationsbekræftelsesdata.

den nationale sikkerhed i fare eller være til skade for menneskers liv og fysiske sikkerhed, kan den imidlertid udsættes ([228]). Underretningen skal ske senest 30 dage efter, at årsagerne til udsættelsen ikke længere gør sig gældende ([229]).

Dette underretningskrav gælder dog kun for indsamling af oplysninger, hvis mindst en af parterne er koreansk statsborger. Som følge heraf vil ikkekoreanske statsborgere kun blive underrettet, når deres kommunikation med koreanske statsborgere indsamles. Der er derfor ikke krav om underretning, når der udelukkende indsamles kommunikation mellem ikkekoreanske statsborgere.

Indholdet af enhver kommunikation samt kommunikationsbekræftelsesdata, der er indsamlet gennem overvågning i henhold til CPPA, må kun anvendes 1) til efterforskning, retsforfølgelse eller forebyggelse af visse former for kriminalitet, 2) i disciplinærsager, 3) i retssager, hvor en part i kommunikationen påberåber sig disse i et erstatningssøgsmål, eller 4) på grundlag af anden lovgivning ([230]).

3.2.1.2. Politiets og anklagerens indsamling af kommunikationsdata til nationale sikkerhedsformål

Politiet og anklageren kan indsamle kommunikationsdata (både kommunikationsindhold og kommunikationsbekræftelsesdata) til nationale sikkerhedsformål på samme betingelser som beskrevet i afsnit 3.2.1.1. I nødsituationer ([231]) anvendes den procedure, der er beskrevet ovenfor, for indsamling af indholdet af kommunikation med henblik på retshåndhævelse i nødsituationer (dvs. artikel 8 i CPPA).

3.2.2. *Indsamling af oplysninger om terrormistænkte*

3.2.2.1. Retsgrundlag

Antiterrorloven giver chefen for NIS beføjelse til at indsamle oplysninger om terrormistænkte ([232]). En »*terrormistænkt*« defineres som et medlem af en terrorgruppe ([233]), en person, der har propaganderet for en terrorgruppe (ved at fremme og udbrede en terrorgruppes idéer eller taktik), rejst eller bidraget til finansiering af terrorisme ([234]) eller deltaget i andre aktiviteter såsom forberedelse, sammensværgelse, udbredelse af propaganda om eller anstiftelse af terrorisme, eller en person, hvor der er begrundet mistanke om, at den pågældende har udført sådanne aktiviteter ([235]). Som hovedregel skal alle offentlige ansatte, der håndhæver antiterrorloven, respektere de grundlæggende rettigheder, der er nedfældet i den koreanske forfatning ([236]).

I antiterrorloven fastsættes der ikke specifikke beføjelser, begrænsninger og garantier for indsamling af oplysninger om terrormistænkte, idet der i stedet henvises til procedurerne i andre love. For det første kan chefen for NIS i henhold til antiterrorloven indsamle 1) oplysninger om indrejse i og udrejse fra Republikken Korea, 2) oplysninger om finansielle transaktioner og 3) oplysninger om kommunikation. Afhængigt af typen af oplysninger, der anmodes om, er de relevante proceduremæssige krav fastsat i henholdsvis immigrationsloven, toldloven, ARUSFTI eller CPPA ([237]). Med hensyn til indsamling af oplysninger om indrejse i og udrejse fra Korea henvises der i antiterrorloven til de procedurer,

([228]) Artikel 9-2, stk. 4, i CPPA.
([229]) Artikel 13-4, stk. 2, og artikel 9-2, stk. 6, i CPPA.
([230]) Artikel 5, stk. 1-2, og artikel 12 og 13-5 i CPPA.
([231]) Hvis foranstaltningen er rettet mod en sammensværgelse, der truer den nationale sikkerhed, og der foreligger en nødsituation, som gør det umuligt at følge den almindelige godkendelsesprocedure (artikel 8, stk. 1, i CPPA).
([232]) Artikel 9 i antiterrorloven.
([233]) En »*terrorgruppe*« defineres som en gruppe terrorister, der er opført på FN's liste (artikel 2, stk. 2, i antiterrorloven).
([234]) »*Terrorisme*« defineres i artikel 2, stk. 1, i antiterrorloven som handlinger, der udføres med det formål at hindre statens, en lokal myndigheds eller en udenlandsk regerings myndighedsudøvelse (herunder lokale myndigheder og internationale organisationer) eller med det formål at tvinge dem til at handle uden nogen forpligtelse hertil eller true offentligheden. Dette omfatter a) drab på en person eller udsættelse af en persons for livsfare ved at forårsage legemsbeskadigelse eller anholdelse, indespærring, kidnapning eller gidseltagning af en person, b) visse former for handlinger rettet mod et luftfartøj (f.eks. sammenstyrtning, kapring eller beskadigelse af et luftfartøj under flyvning), c) visse former for handlinger rettet mod et skib (f.eks. beslaglæggelse af et skib eller en maritim struktur i drift, ødelæggelse af et skib eller en maritim struktur i drift eller beskadigelse heraf i et omfang, der bringer sikkerheden i fare, herunder skader lasten på skibet eller den maritime struktur i drift), d) anbringelse, detonering eller anden anvendelse af et biokemisk, eksplosivt eller brændbart våben eller udstyr med det formål at forårsage død, alvorlig personskade eller alvorlig materiel skade eller at have en sådan indvirkning på visse typer køretøjer eller anlæg (f.eks. tog, sporvogne, motorkøretøjer, offentlige parker og stationer, el- og gasforsyningsanlæg og telekommunikationsanlæg mv.), e) visse former for handlinger i forbindelse med nukleare materialer, radioaktive materialer eller nukleare anlæg (f.eks. skade på menneskers liv, legeme eller ejendom eller forstyrrelse af den offentlige sikkerhed ved at ødelægge en atomreaktor eller forsætligt manipulere radioaktive materialer osv.).
([235]) Artikel 2, stk. 3, i antiterrorloven.
([236]) Artikel 3, stk. 3, i antiterrorloven.
([237]) Artikel 9, stk. 1, i antiterrorloven.

der er fastsat i immigrationsloven og toldloven. Disse love indeholder imidlertid på nuværende tidspunkt ingen bestemmelser om sådanne beføjelser. Med hensyn til indsamling af kommunikationsdata og oplysninger om finansielle transaktioner henvises der i antiterrorloven til begrænsningerne og garantierne i CPPA (som er nærmere beskrevet nedenfor) og ARUSFTI (der som forklaret i afsnit 2.1 ikke er relevant for vurderingen i forbindelse med afgørelsen om tilstrækkeligheden af beskyttelsesniveauet).

Det præciseres ligeledes i artikel 9, stk. 3, i antiterrorloven, at chefen for NIS kan anmode om personoplysninger eller lokaliseringsdata om en terrormistænkt fra en persondataansvarlig ([238]) eller en udbyder af lokaliseringsdata ([239]). Denne mulighed er begrænset til anmodninger om frivillig fremlæggelse af oplysninger, som persondataansvarlige og udbydere af lokaliseringsdata ikke er forpligtet til at efterkomme og under alle omstændigheder kun må efterkomme i overensstemmelse med PIPA og lov om lokaliseringsdata (jf. afsnit 3.2.2.2 nedenfor).

3.2.2.2. Begrænsninger og garantier for frivillig fremlæggelse af oplysninger i henhold til PIPA og lov om lokaliseringsdata

Anmodninger om frivilligt samarbejde i henhold til antiterrorloven skal begrænses til oplysninger om terrormistænkte (jf. afsnit 3.2.2.1 ovenfor). En sådan anmodning fra NIS skal være i overensstemmelse med principperne om lovlighed, nødvendighed og proportionalitet i den koreanske forfatning (artikel 12, stk. 1, og artikel 37, stk. 2) ([240]) samt PIPA-kravene om indsamling af personoplysninger (artikel 3, stk. 1, i PIPA, jf. afsnit 1.2 ovenfor). Det præciseres endvidere i NIS-loven, at NIS ikke må misbruge sine offentlige myndighedsbeføjelser under udførelsen af sine opgaver til at tvinge nogen institution, organisation eller enkeltperson til at gøre noget, som de ikke er forpligtet til, eller hindre en person i at udøve sine rettigheder ([241]). En overtrædelse af dette forbud kan føre til strafferetlige sanktioner ([242]).

Persondataansvarlige og udbydere af lokaliseringsdata, der modtager anmodninger fra NIS på grundlag af antiterrorloven, er ikke forpligtet til at efterkomme sådanne anmodninger. De kan efterkomme dem frivilligt, men kun i overensstemmelse med PIPA og lov om lokaliseringsdata.. Med hensyn til overholdelse af PIPA skal den dataansvarlige navnlig tage hensyn til den registreredes interesser og må ikke videregive oplysningerne, hvis dette sandsynligvis vil krænke den registreredes eller tredjemands interesser uretmæssigt ([243]). Desuden skal den berørte person i henhold til meddelelse nr. 2021-1 om supplerende regler for fortolkning og anvendelse af lov om beskyttelse af personoplysninger underrettes om videregivelsen. Under ekstraordinære omstændigheder kan underretningen udsættes, navnlig hvis og så længe underretningen vil bringe en igangværende strafferetlig efterforskning i fare eller sandsynligvis vil skade en anden persons liv eller legeme, hvis disse rettigheder eller interesser går klart forud for den registreredes rettigheder ([244]).

3.2.2.3. Begrænsninger og garantier i henhold til CPPA

I henhold til antiterrorloven må efterretningsagenturer kun indsamle kommunikationsdata (både kommunikationsindhold og kommunikationsbekræftelsesdata), når det er nødvendigt i forbindelse med terrorbekæmpelsesaktiviteter, dvs. aktiviteter i forbindelse med forebyggelse af og modforanstaltninger mod terrorisme. Procedurerne i CPPA, der er beskrevet i afsnit 3.2.1, finder anvendelse på indsamling af kommunikationsdata med henblik på bekæmpelse af terrorisme.

3.2.3. *Teleoperatørers frivillige videregivelse af oplysninger*

I henhold til TBA kan teleoperatører efterkomme en anmodning om videregivelse af »kommunikationsdata« fra et efterretningsagentur, der agter at indsamle oplysningerne for at forebygge en trussel mod den nationale sikkerhed ([245]). En sådan anmodning skal være i overensstemmelse med principperne om lovlighed, nødvendighed og proportionalitet i den koreanske forfatning (artikel 12, stk. 1, og artikel 37, stk. 2) ([246]) samt PIPA-kravene om indsamling af personoplysninger (artikel 3, stk. 1, i PIPA, jf. afsnit 1.2 ovenfor). Desuden gælder de samme begrænsninger og garantier som for frivillig fremlæggelse af oplysninger med henblik på retshåndhævelse (jf. afsnit 2.2.3) ([247]).

([238]) Som defineret i artikel 2 i PIPA, dvs. en offentlig institution, juridisk person, organisation, fysisk person mv., der behandler personoplysninger direkte eller indirekte for at administrere persondatafiler i officielt øjemed eller forretningsøjemed

([239]) Som defineret i artikel 5 i lov om beskyttelse, anvendelse mv. af lokaliseringsdata »lov om lokaliseringsdata«), dvs. enhver, der har fået tilladelse fra Koreas kommunikationskommission til at arbejde med lokaliseringsdata.

([240]) Se også artikel 3, stk. 2 og 3, i antiterrorloven.

([241]) Artikel 19 i NIS-loven.

([242]) Artikel 11, stk. 1, i NIS-loven

([243]) Artikel 18, stk. 2, i PIPA.

([244]) PIPC-meddelelse nr. 2021-1 om supplerende regler for fortolkning og anvendelse af lov om beskyttelse af personoplysninger, afsnit III, 2, nr. iii).

([245]) Artikel 83, stk. 3, i TBA.

([246]) Se også artikel 3, stk. 2 og 3, i antiterrorloven.

([247]) Anmodningen skal navnlig være skriftlig og indeholde en begrundelse for anmodningen samt linket til den relevante bruger og oplysninger om omfanget af de ønskede data, og teleudbyderen skal føre fortegnelser og aflægge rapport til ministeren for videnskab og IKT to gange om året.

En teleoperatør er ikke forpligtet til at efterkomme anmodningen, men kan gøre dette frivilligt, men kun i overensstemmelse med PIPA. I denne henseende gælder de samme forpligtelser, herunder vedrørende underretning af den berørte person, for teleoperatører, som når de modtager anmodninger fra strafferetlige håndhævelsesmyndigheder, som forklaret nærmere i afsnit 2.2.3.

3.3. **Tilsyn**

Forskellige organer fører tilsyn med de koreanske efterretningsagenturers aktiviteter. Tilsynet med forsvarssikkerhedskommandoen varetages af forsvarsministeriet i henhold til ministeriets direktiv om gennemførelse af intern revision. Den udøvende magt, nationalforsamlingen og andre uafhængige organer fører tilsyn med NIS som forklaret nærmere nedenfor.

3.3.1. *Den ansvarlige for beskyttelse af menneskerettigheder*

I henhold til antiterrorloven skal antiterrorkommissionen og den ansvarlige for beskyttelse af menneskerettigheder (»HRPO«) føre tilsyn med efterretningsagenturers indsamling af oplysninger om terrormistænkte ([248]).

Antiterrorkommissionen udvikler bl.a. politikker vedrørende terrorbekæmpelsesaktiviteter og fører tilsyn med gennemførelsen af terrorbekæmpelsesforanstaltninger samt de forskellige kompetente myndigheders aktiviteter på terrorbekæmpelsesområdet ([249]). Kommissionen ledes af premierministeren og består af flere ministre og myndighedschefer, herunder udenrigsministeren, justitsministeren, forsvarsministeren, indenrigs- og sikkerhedsministeren, chefen for NIS, generalkommissæren for det nationale politiagentur og formanden for kommissionen for finansielle tjenesteydelser ([250]). Chefen for NIS skal rapportere til formanden for antiterrorkommissionen (dvs. premierministeren) om efterforskninger af terrorisme og sporingen af terrormistænkte for at indsamle de nødvendige oplysninger eller materialer til terrorbekæmpelsesaktiviteter ([251]).

Antiterrorloven indfører endvidere HRPO'en for at beskytte personers grundlæggende rettigheder mod krænkelser i forbindelse med terrorbekæmpelsesaktiviteter ([252]). HRPO'en udnævnes af formanden for antiterrorkommissionen blandt personer, der opfylder kvalifikationskriterierne anført i gennemførelsesdekretet til antiterrorloven (dvs. enhver, der har udøvet hvervet som advokat og har mindst ti års erhvervserfaring, eller har ekspertviden på menneskerettighedsområdet og arbejder eller har arbejdet (som minimum) på lektorniveau i mindst ti år, eller har bestridt en højere embedsmandsstilling i statsforvaltninger eller lokale myndigheder eller har mindst ti års erhvervserfaring på menneskerettighedsområdet, f.eks. i en ikkestatslig organisation) ([253]). HRPO'en udnævnes for to år (med mulighed for en ny embedsperiode) og kan kun afsættes af specifikke, begrænsede grunde, og hvis det er berettiget, f.eks. når der er rejst tiltale i en straffesag i forbindelse med vedkommendes opgaver, i forbindelse med videregivelse af fortrolige oplysninger eller på grund af langvarig psykisk eller fysisk sygdom ([254]).

Med hensyn til beføjelser kan HRPO udstede henstillinger om forbedringer af beskyttelsen af menneskerettighederne i agenturer, der er involveret i terrorbekæmpelsesaktiviteter, og behandle civile klager (jf. afsnit 3.4.3) ([255]). Hvis det med rimelighed kan fastslås, at der er sket en krænkelse af menneskerettighederne i forbindelse med udøvelsen af officielle pligter, kan HRPO henstille til chefen for det ansvarlige agentur at rette op på en sådan overtrædelse ([256]). Det ansvarlige agentur skal efterfølgende give HRPO meddelelse om de foranstaltninger, der er truffet for at gennemføre en sådan henstilling ([257]). Hvis et agentur ikke gennemfører en henstilling fra HRPO, vil sagen blive rejst over for kommissionen, herunder dens formand, premierministeren. Der har ikke hidtil været tilfælde, hvor henstillingerne fra HRPO ikke er blevet gennemført.

3.3.2. *Nationalforsamlingen*

Som beskrevet i afsnit 2.3.2 kan nationalforsamlingen undersøge og inspicere offentlige myndigheder og i denne forbindelse anmode om fremlæggelse af dokumenter og pålægge vidner at give møde. For så vidt angår anliggender, der henhører under NIS' kompetenceområde, udføres denne parlamentariske kontrol af nationalforsamlingens

([248]) Artikel 7 i antiterrorloven.
([249]) Artikel 5, stk. 3, i antiterrorloven.
([250]) Artikel 3, stk. 1, i gennemførelsesdekretet til antiterrorloven.
([251]) Artikel 9, stk. 4, i antiterrorloven.
([252]) Artikel 7 i antiterrorloven.
([253]) Artikel 7, stk. 1, i gennemførelsesdekretet til antiterrorloven.
([254]) Artikel 7, stk. 3, i gennemførelsesdekretet til antiterrorloven.
([255]) Artikel 8, stk. 1, i gennemførelsesdekretet til antiterrorloven.
([256]) Artikel 9, stk. 1, i gennemførelsesdekretet til antiterrorloven. HRPO træffer selv afgørelse om vedtagelsen af henstillinger, men skal rapportere sådanne henstillinger til formanden for antiterrorkommissionen.
([257]) Artikel 9, stk. 2, i gennemførelsesdekretet til antiterrorloven.

efterretningsudvalg ([258]). Chefen for NIS, som fører tilsyn med agenturets varetagelse af sine opgaver, rapporterer til efterretningsudvalget (samt til præsidenten) ([259]). Efterretningsudvalget kan også selv anmode om en rapport om et specifikt spørgsmål, som chefen for NIS straks skal reagere på ([260]). Chefen kan kun nægte at svare eller afgive vidneforklaring i efterretningsudvalget, når der er tale om statshemmeligheder om militære, diplomatiske eller nordkoreanske spørgsmål, hvor offentlighedens kendskab kan have en alvorlig indvirkning på den nationale skæbne ([261]). I så fald kan efterretningsudvalget anmode premierministeren om en forklaring. Hvis der ikke gives en forklaring senest syv dage efter indgivelsen af anmodningen, kan svaret eller vidneforklaringen ikke længere afslås.

Hvis nationalforsamlingen konkluderer, at der har fundet ulovlige eller uretmæssige aktiviteter sted, kan den anmode den relevante offentlige myndighed om at træffe korrigerende foranstaltninger, herunder tilkende erstatning, iværksætte disciplinære foranstaltninger og forbedre sine interne procedurer ([262]). Efter en sådan anmodning skal myndigheden handle straks og aflægge rapport om resultatet til nationalforsamlingen. Der findes særlige regler for parlamentarisk kontrol med anvendelsen af kommunikationsbegrænsende foranstaltninger (dvs. indsamling af indholdet af kommunikation) i henhold til CCPA ([263]). For så vidt angår sidstnævnte kan nationalforsamlingen anmode lederne af efterretningsagenturerne om en rapport om enhver specifik kommunikationsbegrænsende foranstaltning. Den kan desuden foretage inspektion på stedet af aflytningsudstyr. Endelig skal efterretningsagenturer, der har indsamlet, og operatører, der har videregivet indholdsoplysninger til nationale sikkerhedsformål, indberette sådanne oplysninger efter anmodning fra nationalforsamlingen.

3.3.3. *Revisions- og inspektionsudvalget*

BAI udfører de samme tilsynsfunktioner i forhold til efterretningsagenturer som inden for strafferetlig håndhævelse (jf. afsnit 2.3.2) ([264]).

3.3.4. *Kommissionen for beskyttelse af personoplysninger*

Hvad angår databehandling til nationale sikkerhedsformål, herunder i indsamlingsfasen, fører PIPC yderligere tilsyn. Som forklaret nærmere i afsnit 1.2 omfatter dette de generelle principper og forpligtelser, der er fastsat i artikel 3 og artikel 58, stk. 4, i PIPA, samt udøvelsen af de individuelle rettigheder, der er garanteret ved artikel 4 i PIPA. I henhold til artikel 7-8, stk. 3 og 4, og artikel 7-9, stk. 5, i PIPA omfatter PIPC's tilsyn desuden mulige overtrædelser af reglerne i specifikke love, der fastsætter begrænsninger og garantier for indsamling af personoplysninger, såsom CPPA, antiterrorloven og TBA. I betragtning af kravene i artikel 3, stk. 1, i PIPA om lovlig og rimelig indsamling af personoplysninger udgør enhver overtrædelse af disse love en overtrædelse af PIPA. PIPC har således beføjelse til at undersøge ([265]) overtrædelser af lovgivningen om adgang til oplysninger til nationale sikkerhedsformål og reglerne for behandling i PIPA og fremsætte henstillinger om forbedringer, pålægge korrigerende foranstaltninger, henstille, at der træffes disciplinære foranstaltninger, og henvise potentielle lovovertrædelser til de relevante efterforskningsmyndigheder ([266]).

3.3.5. *Den nationale menneskerettighedskommission*

NRHC fører tilsyn med efterretningsagenturer på samme måde som med andre statslige myndigheder (jf. afsnit 2.3.2).

3.4. **Individuel klage- og prøvelsesadgang**

3.4.1. *Klageadgang for den ansvarlige for beskyttelse af menneskerettigheder*

Med hensyn til indsamling af personoplysninger i forbindelse med terrorbekæmpelsesaktiviteter stiller HRPO, der er oprettet under antiterrorkommissionen, en særlig klagemulighed til rådighed. HRPO behandler civile klager vedrørende krænkelse af menneskerettighederne i forbindelse med terrorbekæmpelsesaktiviteter ([267]). HRPO'en kan henstille, at der træffes korrigerende foranstaltninger, og det pågældende organ skal underrette HRPO'en om enhver foranstaltning, der træffes for at gennemføre en sådan henstilling. Der er intet krav om umiddelbarklageberettigelse for personer, der ønsker at indgive en klage til HRPO. Som følge heraf behandler HRPO klagen, selv om den pågældende person ikke kan påvise en faktisk skade på tidspunktet for antagelsen.

([258]) Se også artikel 36 og artikel 37, stk. 1, nr. 16, i lov om nationalforsamlingen.
([259]) Artikel 18 i NIS-loven.
([260]) Artikel 15, stk. 2, i NIS-loven
([261]) Artikel 17, stk. 2, i NIS-loven »Statshemmeligheder« defineres som »*kendsgerninger, varer eller viden, der er klassificeret som statshemmeligheder, og hvortil adgang kun er tilladt for et begrænset antal personer, og som ikke må videregives til andre lande eller organisationer for at undgå alvorlige indvirkninger på den nationale sikkerhed*«, jf. artikel 13, stk. 4, i NIS-loven.
([262]) Artikel 16, stk. 2, i lov om inspektion og undersøgelse af statsforvaltningen.
([263]) Artikel 15 i CPPA.
([264]) Som det er tilfældet med nationalforsamlingens efterretningsudvalg, kan chefen for NIS kun nægte at svare BAI, hvis der er tale om statshemmeligheder, og offentlighedens kendskab hertil ville have en alvorlig indvirkning på den nationale sikkerhed (artikel 13, stk. 1, i NIS-loven).
([265]) Artikel 63 i PIPA.
([266]) Artikel 61, stk. 2, artikel 65, stk. 1, artikel 65, stk. 2, og artikel 64, stk. 4.
([267]) Artikel 8, stk. 1, nr. 2, i gennemførelsesdekretet til antiterrorloven.

3.4.2. *Prøvelsesmekanismer i henhold til PIPA*

Enkeltpersoner kan udøve deres ret til indsigt i og berigtigelse, sletning og suspension i henhold til PIPA af personoplysninger, der behandles til nationale sikkerhedsformål ([268]). Anmodninger om udøvelse af disse rettigheder kan indgives direkte til efterretningstjenesten eller indirekte via PIPC. Efterretningsagenturet kan udsætte, begrænse eller nægte udøvelsen af en sådan rettighed, i det omfang og så længe det er nødvendigt og forholdsmæssigt for at beskytte et vigtigt mål af samfundsmæssig interesse (f.eks. i det omfang og så længe indrømmelsen af rettigheden vil bringe en igangværende efterforskning i fare eller true den nationale sikkerhed), eller hvis indrømmelsen af rettigheden kan skade tredjemands liv eller legeme. Hvis anmodningen afslås eller begrænses, skal den pågældende straks underrettes om årsagerne hertil.

I overensstemmelse med artikel 58, stk. 4, i PIPA (krav om at sikre en korrekt behandling af individuelle klager) og artikel 4, stk. 5, i PIPA (retten til passende erstatning for enhver skade, der opstår som følge af behandlingen af personoplysninger, gennem en hurtig og retfærdig procedure) har enkeltpersoner desuden ret til at få prøvet deres sag. Dette omfatter retten til at indberette en påstået overtrædelse til callcentret for privatlivsbeskyttelse, der drives af Koreas internet- og sikkerhedsagentur, og indgive en klage til PIPC ([269]). Disse prøvelsesmekanismer er tilgængelige både i tilfælde af mulige overtrædelser af reglerne i specifikke love, der fastsætter begrænsninger og garantier for indsamling af personoplysninger til nationale sikkerhedsformål, og i PIPA. Som forklaret i meddelelse nr. 2021-1 kan en EU-borger indgive en klage til PIPC via sin nationale databeskyttelsesmyndighed. I så fald underretter PIPC den pågældende via den nationale databeskyttelsesmyndighed, når undersøgelsen er afsluttet (herunder, hvis det er relevant, med oplysninger om de pålagte korrigerende foranstaltninger). PIPC's afgørelser eller manglende handling kan endvidere indbringes for de koreanske domstole i henhold til lov om forvaltningssager.

3.4.3. *Klageadgang ved den nationale menneskerettighedskommission*

Muligheden for at indbringe en individuel klage for NHRC gælder på samme måde for efterretningsagenturer som for andre statslige myndigheder (jf. afsnit 2.4.2).

3.4.4. *Retslig prøvelse*

Som det er tilfældet med strafferetlige håndhævelsesmyndigheders aktiviteter, har enkeltpersoner forskellige muligheder for at anlægge sag mod efterretningsagenturer i forbindelse med overtrædelser af ovennævnte begrænsninger og garantier.

For det første kan enkeltpersoner opnå skadeserstatning efter lov om erstatning fra staten. I en sag blev der f.eks. ydet erstatning for ulovlig overvågning foretaget af forsvarsstøttekommandoen (forgængeren for forsvarssikkerhedskommandoen) ([270]).

For det andet giver lov om forvaltningssager enkeltpersoner mulighed for at anfægte forvaltningsorganers, herunder efterretningsagenturers, dispositioner og undladelser ([271]).

Endelig kan enkeltpersoner indgive en forfatningsmæssig klage til forfatningsdomstolen over foranstaltninger truffet af efterretningsagenturer på grundlag af lov om forfatningsdomstolen.

([268]) Artikel 3, stk. 5, og artikel 4, stk. 1. 3 og 4, i PIPA.
([269]) Artikel 62 og artikel 63, stk. 2, i PIPA.
([270]) Højesterets afgørelse nr. 96Da42789 af 24. juli 1998.
([271]) Artikel 3 og 4 i lov om forvaltningssager.

ISSN 1977-0634 (elektronisk udgave)
ISSN 1725-2520 (papirudgave)

Den Europæiske Unions Publikationskontor
L-2985 Luxembourg
LUXEMBOURG

DA