FORORDNINGER

KOMMISSIONENS FORORDNING (EU) Nr. 611/2013

af 24. juni 2013

om de foranstaltninger, der skal anvendes ved underretningen om brud på persondatasikkerheden, jf. Europa-Parlamentets og Rådets direktiv 2002/58/EF vedrørende databeskyttelse inden for elektronisk kommunikation

EUROPA-KOMMISSIONEN HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Europa-Parlamentets og Rådets direktiv 2002/58/EF af 12. juli 2002 om behandling af personoplysninger og beskyttelse af privatlivets fred i den elektroniske kommunikationssektor (Direktiv om databeskyttelse inden for elektronisk kommunikation) [1], særlig artikel 4, stk. 5,

efter at have hørt Det Europæiske Agentur for Net- og Informationssikkerhed (ENISA),

efter at have hørt Gruppen vedrørende Beskyttelse af Personer i forbindelse med Behandling af Personoplysninger, der er nedsat ved artikel 29 i Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger [2] (Artikel 29-Gruppen),

efter høring af Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) og

ud fra følgende betragtninger:

(1) Direktiv 2002/58/EF tager sigte på en harmonisering af nationale bestemmelser, der er nødvendig for at sikre et ensartet niveau i beskyttelsen af de grundlæggende rettigheder og frihedsrettigheder og navnlig retten til privatlivets fred og fortrolighed i forbindelse med behandling af personoplysninger inden for den elektroniske kommunikationssektor og for at sikre fri omsætning af sådanne oplysninger og af elektronisk kommunikationsudstyr og elektroniske kommunikationstjenester i Unionen.

(2) I henhold til artikel 4 i direktiv 2002/58/EF har udbydere af offentligt tilgængelige kommunikationstjenester pligt til at underrette de kompetente nationale myndigheder og i visse tilfælde også berørte abonnenter og fysiske personer om brud på persondatasikkerheden. Brud på persondatasikkerheden er i artikel 2, litra i), i direktiv 2002/58/EF defineret som et sikkerhedsbrud, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, ubeføjet videregivelse af eller adgang til persondata, der sendes, lagres eller på anden måde behandles i forbindelse med udbuddet af offentligt tilgængelige kommunikationstjenester i Unionen.

(3) For at sikre en ensartet gennemførelse af de foranstaltninger, der er anført i artikel 4, stk. 2, 3 og 4, i direktiv 2002/58/EF, giver samme direktivs artikel 4, stk. 5, Kommissionen beføjelse til at vedtage tekniske gennemførelsesforanstaltninger om, under hvilke omstændigheder informations- og underretningskravene i denne artikel gælder, samt hvilke former og procedurer der skal anvendes.

(4) Forskelle i nationale krav i denne henseende kan medføre retlig usikkerhed, mere komplicerede og omstændelige procedurer og betydelige administrative omkostninger for udbydere, der opererer på tværs af landegrænserne. Kommissionen finder det derfor nødvendigt at vedtage sådanne tekniske gennemførelsesforanstaltninger.

(5) Denne forordning er afgrænset til at omhandle underretningen om brud på persondatasikkerheden, og der er derfor ikke fastsat tekniske gennemførelsesforanstaltninger for artikel 4, stk. 2, i direktiv 2002/58/EF om underretning af abonnenter i tilfælde af en særlig risiko for brud på netsikkerheden.

(6) Det følger af første afsnit i artikel 4, stk. 3, i direktiv 2002/58/EF, at udbyderne skal underrette den kompetente nationale myndighed om alle brud på persondatasikkerheden. Der bør derfor ikke overlades skønsbeføjelser til udbyderen om, hvorvidt den kompetente myndighed bør underrettes. Dette bør dog ikke hindre den berørte kompetente nationale myndighed i at prioritere undersøgelsen af visse brud på den måde, som den finder passende i overensstemmelse med den gældende lovgivning, og om fornødent at træffe foranstaltninger for at undgå over- eller underrapportering om brud på persondatasikkerheden.

(7) Der bør tilvejebringes en ordning for underretning om brud på persondatabeskyttelsen til den kompetente nationale myndighed, og når visse betingelser er opfyldt, bør ordningen bestå af forskellige faser, som hver især er omfattet af visse frister. Hensigten med ordningen er at sikre, at den kompetente nationale myndighed underrettes så hurtigt og så fyldestgørende som muligt uden dog på en urimelig måde at hindre udbyderen i sine bestræbelser på at undersøge bruddet og træffe de nødvendige foranstaltninger for at begrænse det og afbøde konsekvenserne heraf.

[1] EFT L 201 af 31.7.2002, s. 37.
[2] EFT L 281 af 23.11.1995, s. 31.

(8) Hverken en simpel formodning om, at et brud på persondatasikkerheden har fundet sted, eller en simpel påvisning af en hændelse, hvis de disponible oplysninger er utilstrækkelige trods det, at en udbyder gør sit bedste for at skabe afklaring, er tilstrækkeligt til at anse et brud på persondatasikkerheden for at være påvist i denne forordnings forstand. Der bør i den forbindelse tages særligt hensyn til, om de oplysninger, der er nævnt i bilag I, står til rådighed.

(9) De berørte kompetente nationale myndigheder bør samarbejde om anvendelsen af denne forordning i tilfælde, hvor et brud på persondatasikkerheden har en tværnational dimension.

(10) I denne forordning foretages der ingen yderligere specifikation af de optegnelser over brud på persondatasikkerheden, som udbydere fører, fordi indholdet specificeres udtømmende i artikel 4 i direktiv 2002/58/EF. Udbydere kan dog benytte nærværende forordning med henblik på at fastlægge optegnelsernes format.

(11) Alle kompetente nationale myndigheder bør stille sikre elektroniske midler til rådighed for udbyderne, således at de kan underrette om brud på persondatasikkerheden i et fælles format baseret på en standard som f.eks. XML, med de oplysninger, der er anført i bilag I, på de relevante sprog, så alle udbydere i Unionen kan følge en ensartet underretningsprocedure, uanset hvor de befinder sig, eller hvor bruddet på persondatasikkerheden fandt sted. Kommissionen bør i den forbindelse lette gennemførelsen af de sikre elektroniske midler ved om fornødent at indkalde de kompetente nationale myndigheder til møder.

(12) Ved vurderingen af, om et brud på persondatasikkerheden kan forventes at krænke personoplysninger eller privatlivets fred for en abonnent eller en fysisk person, bør der tages hensyn til bl.a. karakteren og indholdet af de pågældende personoplysninger, navnlig hvis oplysningerne vedrører finansielle oplysninger og herunder kreditkortoplysninger og bankoplysninger; særlige kategorier af oplysninger, jf. artikel 8, stk. 1, i direktiv 95/46/EF; og visse data, der specifikt vedrører udbuddet af telefoni- eller internettjenester, dvs. e-maildata, lokaliseringsdata, internetlogfiler, browserhistorik og udspecificerede opkaldslister.

(13) I undtagelsestilfælde bør udbyderen have mulighed for at udskyde underretningen af abonnenten eller den fysiske person, hvis underretningen af abonnenten eller den fysiske person kan bringe en behørig undersøgelse af bruddet på persondatasikkerheden i fare. I denne sammenhæng kan undtagelsestilfælde omfatte strafferetlig efterforskning samt andre brud på persondatasikkerheden, hvor der ikke er tale om en grov forbrydelse, men for hvilke det kan være hensigtsmæssigt at udskyde underretningen. Under alle omstændigheder bør det være op til den kompetente nationale myndighed ud fra det enkelte tilfælde og på baggrund af omstændighederne at tage stilling til, hvorvidt den samtykker i at udskyde underretningen, eller om underretningen skal kræves foretaget.

(14) Udbydere må forventes at have rådighed over deres abonnenters kontaktoplysninger i lyset af deres direkte kontraktforhold, men sådanne oplysninger findes muligvis ikke for andre fysiske personer, der berøres af bruddet på persondatasikkerheden. I det tilfælde bør der gives tilladelse til, at udbyderen i første omgang underretter disse fysiske personer via annoncer i større nationale eller regionale medier, f.eks. aviser, og at disse hurtigst muligt efterfølges af en individuel underretning som fastsat ved denne forordning. Udbyderen forpligtes derfor ikke til at underrette gennem medierne, men får snarere beføjelse til at handle på denne måde, hvis udbyderen ønsker det, når vedkommende stadig er i færd med at identificere alle fysiske personer.

(15) Oplysningerne om bruddet bør stå alene og ikke gives sammen med oplysninger om andre emner. Det betragtes eksempelvis ikke som et velegnet middel til at underrette om et brud på persondatasikkerheden, hvis en normal faktura benyttes til at underrette om et brud på persondatasikkerheden.

(16) Ved denne forordning fastsættes der ikke specifikke tekniske beskyttelsesforanstaltninger, som kan begrunde en fravigelse af pligten til at underrette abonnenter eller fysiske personer om et brud på persondatasikkerheden, fordi disse kan ændre sig med tiden i takt med teknologiske fremskridt. Kommissionen forventer dog at kunne offentliggøre en vejledende liste over sådanne specifikke tekniske beskyttelsesforanstaltninger i henhold til den aktuelle praksis.

(17) Gennemførelse af kryptering eller hashing bør ikke i sig selv betragtes som tilstrækkeligt til, at udbydere generelt kan gøre gældende, at de har opfyldt den generelle sikkerhedsforpligtelse, der er fastsat ved artikel 17 i direktiv 95/46/EF. I den henseende bør udbydere også gennemføre passende organisatoriske og tekniske foranstaltninger, der skal forebygge, påvise og blokere brud på datasikkerheden. Efter at have gennemført kontrolforanstaltninger bør udbydere tage højde for eventuelle tilbageværende risici for at erkende, hvor brud på persondatasikkerheden potentielt kan forekomme.

(18) Benytter udbyderen en anden udbyder til at udføre en del af tjenesteydelsen, f.eks. i forbindelse med fakturering og

ledelsesfunktioner, bør denne anden udbyder, som ikke har et direkte kontraktforhold til slutbrugeren, ikke være forpligtet til at udstede underretninger i tilfælde af brud på persondatasikkerheden. Den anden udbyder bør i stedet advare og oplyse udbyderen, med hvilken vedkommende har indgået et direkte kontraktforhold. Dette bør også gælde i forbindelse med engrosudbud af elektroniske kommunikationstjenester, hvor engrosudbyderen normalt ikke har et direkte kontraktforhold til slutbrugeren.

(19) I direktiv 95/46/EF defineres en generel ramme for beskyttelse af persondata i Den Europæiske Union. Kommissionen har forelagt et forslag til en forordning udstedt af Europa-Parlamentet og Rådet med henblik på at erstatte direktiv 95/46/EF (databeskyttelsesforordningen). Med den foreslåede databeskyttelsesforordning pålægges alle dataansvarlige at underrette om brud på persondatasikkerheden med udgangspunkt i artikel 4, stk. 3, i direktiv 2002/58/EF. Den aktuelle kommissionsforordning er i fuld overensstemmelse med denne foreslåede foranstaltning.

(20) I den foreslåede databeskyttelsesforordning foretages endvidere et begrænset antal tekniske tilpasninger af direktiv 2002/58/EF for at tage højde for, at direktiv 95/46/EF omdannes til en forordning. Kommissionen vil gøre den nye forordnings materielle retlige konsekvenser for direktiv 2002/58/EF til genstand for en ny gennemgang.

(21) Anvendelsen af denne forordning bør tages op til fornyet overvejelse tre år efter ikrafttrædelsen, og dens indhold tages op til fornyet overvejelse i lyset af den gældende lovramme til sin tid og herunder den foreslåede databeskyttelsesforordning. Den fornyede gennemgang af nærværende forordning bør derfor så vidt muligt knyttes sammen med gennemgangen af direktiv 2002/58/EF.

(22) Forordningens anvendelse kan bl.a. vurderes på grundlag af de kompetente nationale medlemsstaters eventuelle statistikker over brud på persondatasikkerheden, som de får underretning om. Disse statistikker kan f.eks. omfatte oplysninger om antallet af brud på persondatasikkerheden, som den kompetente nationale myndighed har modtaget underretning om, antal brud på persondatasikkerheden, som abonnenten eller den fysiske person har modtaget underretning om, den tid, det tager at afhjælpe bruddet på persondatasikkerheden, og hvorvidt der er truffet tekniske beskyttelsesforanstaltninger. Disse statistikker bør give Kommissionen og medlemsstaterne sammenhængende og sammenlignelige statistiske data, og de bør ikke afsløre identiteten af hverken de udbydere, som foretager underretningen, eller abonnenter og fysiske personer. Kommissionen kan også holde jævnlige møder med de kompetente nationale myndigheder og andre interesseparter herom.

(23) Foranstaltningerne i denne forordning er i overensstemmelse med udtalelse fra Kommunikationsudvalget —

VEDTAGET DENNE FORORDNING:

Artikel 1

Genstand

Denne forordning gælder for underretningen om brud på persondatasikkerheden, der foretages af udbydere af offentligt tilgængelige kommunikationstjenester (»udbyderen«).

Artikel 2

Underretning af den kompetente nationale myndighed

1. Udbyderen skal underrette den kompetente nationale myndighed om samtlige brud på persondatasikkerheden.

2. Udbyderen skal underrette den kompetente nationale myndighed om bruddet på persondatabeskyttelsen senest 24 timer efter, at bruddet er påvist, når dette er praktisk muligt.

Udbyderen skal i sin underretning af den kompetente nationale myndighed vedlægge de oplysninger, der er angivet i bilag I.

Et brud på persondatasikkerheden skal anses for at være påvist, hvis en udbyder har opnået tilstrækkelig kendskab til, at en sikkerhedshændelse er indtruffet, og at den har kompromitteret persondatasikkerheden, således at der kan afgives en hensigtsmæssig underretning som krævet ifølge denne forordning.

3. Udbyderen må foretage en indledende underretning af den kompetente nationale myndighed senest 24 timer efter påvisning af bruddet på persondatabeskyttelsen, hvis alle de i bilag I angivne oplysninger ikke foreligger, og der er behov for yderligere efterforskning af bruddet på persondatasikkerheden. Denne indledende underretning af den kompetente nationale myndighed skal indeholde de oplysninger, der er anført i bilag I, afdeling 1. Udbyderen skal foretage en anden underretning af den kompetente nationale myndighed så hurtigt som muligt og senest tre dage efter den indledende underretning. Denne anden underretning skal indeholde de oplysninger, der er anført i bilag I, afdeling 2, og om nødvendigt ajourføre de oplysninger, der allerede er afgivet.

Hvis udbyderen på trods af sin efterforskning ikke er i stand til at forelægge alle oplysninger senest tre dage efter den indledende underretning, skal udbyderen afgive alle disponible oplysninger inden for denne tidsfrist og forelægge den kompetente nationale myndighed en begrundelse for den forsinkede underretning om de resterende oplysninger. Udbyderen forelægger hurtigst muligt de resterende oplysninger for den kompetente nationale myndighed og ajourfører om nødvendigt de oplysninger, der allerede er afgivet.

4. Den kompetente nationale myndighed stiller sikre elektroniske midler til rådighed, således at alle udbydere, der er etableret i den pågældende medlemsstat, kan underrette om brud på persondatasikkerheden, tillige med oplysninger om procedurerne for adgang og brug af denne. Ved behov indkalder Kommissionen til møder mellem de kompetente nationale myndigheder med henblik på at lette anvendelsen af denne bestemmelse.

5. Når bruddet på persondatasikkerheden krænker abonnenter eller fysiske personer fra andre medlemsstater end den kompetente nationale myndigheds medlemsstat, hvori der er underrettet om bruddet på persondatasikkerheden, informerer den kompetente nationale myndighed de øvrige berørte nationale myndigheder.

For at lette anvendelsen af denne bestemmelse opretter og ajourfører Kommissionen en liste over de kompetente nationale myndigheder og de relevante kontaktpunkter.

Artikel 3

Underretning af en abonnent eller en fysisk person

1. Hvis bruddet på persondatasikkerheden kan forventes at krænke personoplysninger eller privatlivets fred for en abonnent eller en fysisk person, skal udbyderen foruden den underretning, der er nævnt i artikel 2, også underrette abonnenten eller den fysiske person om bruddet.

2. Ved vurderingen af, hvorvidt et brud på persondatasikkerheden kan forventes at krænke personoplysninger eller privatlivets fred for en abonnent eller en fysisk person, skal der tages hensyn til bl.a. følgende forhold:

a) karakteren og indholdet af de pågældende personoplysninger, navnlig hvor oplysningerne vedrører finansielle oplysninger, særlige kategorier af oplysninger, jf. artikel 8, stk. 1, i direktiv 95/46/EF, samt lokaliseringsdata, internetlogfiler, browserhistorik, e-maildata og udspecificerede opkaldslister

b) de sandsynlige følger af bruddet på persondatasikkerheden for den berørte abonnent eller fysiske person, navnlig hvis bruddet kan medføre identitetstyveri eller svig, fysisk skade, psykologisk forstyrrelse, tort eller skade af omdømme og

c) omstændighederne ved bruddet på persondatasikkerheden, navnlig når oplysningerne er blevet stjålet, eller når udbyderen er bekendt med, at de nødvendige data er i en uautoriseret tredjemands besiddelse.

3. Abonnenten eller den fysiske person skal underrettes uden unødig forsinkelse, efter at bruddet på persondatasikkerheden er påvist, jf. artikel 2, stk. 2, tredje afsnit. Dette må ikke afhænge af underretningen om bruddet på persondatabeskyttelsen til den kompetente nationale myndighed, der er omhandlet i artikel 2.

4. I udbyderens underretning til abonnenten eller den fysiske person vedlægges de oplysninger, der er fastsat i bilag II. Underretningen af abonnenten eller den fysiske person skal være udtrykt i et klart og letforståeligt sprog. Udbyderen må ikke bruge underretningen som en lejlighed til at fremme eller reklamere for nye eller supplerende tjenester.

5. I undtagelsestilfælde, hvor underretningen af abonnenten eller den fysiske person kan bringe en behørig efterforskning af bruddet på persondatasikkerheden i fare, skal udbyderen efter at have opnået samtykke fra den kompetente nationale myndighed gives tilladelse til at udskyde underretningen af abonnenten eller den fysiske person, indtil den kompetente nationale myndighed skønner det muligt at underrette om bruddet på persondatasikkerheden i overensstemmelse med denne artikel.

6. Udbyderen skal underrette abonnenten eller den fysiske person om bruddet på persondatasikkerheden med kommunikationsmidler, som sikrer en hurtig modtagelse af oplysningerne, og som er sikret i overensstemmelse med aktuelle teknikker. Oplysningerne om bruddet skal stå alene og må ikke gives sammen med oplysninger om andre emner.

7. Hvis udbyderen, som har et direkte kontraktforhold til slutbrugeren, på trods af rimelige bestræbelser er ude af stand til inden for den tidsfrist, der er angivet i stk. 3, at identificere alle fysiske personer, som må forventes at blive krænket af bruddet på persondatasikkerheden, kan udbyderen underrette disse personer gennem annoncer i større nationale eller regionale medier i de relevante medlemsstater inden for tidsfristen. Disse annoncer skal indeholde de oplysninger, der er angivet i bilag II, om nødvendigt i sammenfattet form. I dette tilfælde skal udbyderen videreføre rimelige bestræbelser på at identificere disse fysiske personer og underrette dem om de i bilag II angivne oplysninger hurtigst muligt.

Artikel 4

Tekniske beskyttelsesforanstaltninger

1. Uanset artikel 3, stk. 1, er det ikke nødvendigt at underrette den pågældende abonnent eller fysiske person om et brud på persondatasikkerheden, hvis den kompetente nationale myndighed finder det godtgjort fra udbyderens side, at denne har gennemført passende teknologiske beskyttelsesforanstaltninger, og at disse foranstaltninger er blevet anvendt på de data, som sikkerhedsbruddet vedrørte. Sådanne teknologiske beskyttelsesforanstaltninger skal gøre dataene uforståelige for alle, der ikke har lovlig adgang hertil.

2. Data anses for uforståelige, hvis:

a) de er blevet krypteret på sikker vis med en standardiseret algoritme, dekrypteringsnøglen ikke er kompromitteret af et brud på sikkerheden, og dekrypteringsnøglen er genereret på en sådan måde, at den ikke kan afsløres med de tilgængelige tekniske midler af en person, der ikke har lovlig adgang til nøglen eller

b) de er blevet erstattet af deres hashværdi, der beregnes med en standardiseret kryptografisk hashfunktion med en nøgle, den nøgle, der er anvendt til at hashe dataene, ikke er kompromitteret af et brud på sikkerheden, og den nøgle, der er anvendt til at hashe dataene, er genereret på en sådan måde, at den ikke kan afsløres med de tilgængelige tekniske midler af en person, der ikke har lovlig adgang til nøglen.

3. Kommissionen kan efter at have hørt de kompetente nationale myndigheder via Artikel 29-Gruppen, Det Europæiske Agentur for Net- og Informationssikkerhed og Den Europæiske Tilsynsførende for Databeskyttelse offentliggøre en vejledende liste over egnede tekniske beskyttelsesforanstaltninger som nævnt i stk. 1 i overensstemmelse med den gældende praksis.

Artikel 5

Anvendelse af en anden udbyder

Indgår en udbyder en kontrakt med en anden udbyder om at levere en del af de elektroniske kommunikationstjenester uden at have et direkte kontraktforhold til abonnenter, skal denne anden udbyder øjeblikkeligt oplyse den kontraherende udbyder om brud på persondatasikkerheden.

Artikel 6

Rapportering og fornyet gennemgang

Inden for tre år efter denne forordnings ikrafttræden skal Kommissionen forelægge en rapport om forordningens anvendelse, dens effektivitet og konsekvenser for udbydere, abonnenter og fysiske personer. På grundlag af denne rapport foretager Kommissionen en fornyet gennemgang af denne forordning.

Artikel 7

Ikrafttræden

Denne forordning træder i kraft den 25. august 2013.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 24. juni 2013.

På Kommissionens vegne
José Manuel BARROSO
Formand

BILAG I

Indholdet af underretningen til den kompetente nationale myndighed

Afdeling 1

Udbyderens identitet

1. Udbyderens navn

2. Identitet og kontaktoplysninger for den databeskyttelsesansvarlige eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes

3. Hvorvidt det drejer sig om den første eller anden underretning

Indledende oplysninger om bruddet på persondatasikkerheden (suppleres i senere underretninger, hvis det er relevant)

4. Dato og tidspunkt for hændelsen (hvis dette er kendt; om nødvendigt kan der gives et skøn) og for påvisningen af hændelsen

5. Omstændighederne ved bruddet på persondatasikkerheden (f.eks. bortkomst, tyveri, kopiering)

6. Karakter og indhold af de berørte personoplysninger

7. Tekniske og organisatoriske foranstaltninger, som udbyderen anvender (eller vil anvende), i henseende til de berørte personoplysninger

8. Relevant anvendelse af andre udbydere (eventuelt)

Afdeling 2

Yderligere oplysninger om bruddet på persondatasikkerheden

9. Resumé af den hændelse, der forårsagede bruddet på persondatasikkerheden (herunder det fysiske sted, hvor bruddet fandt sted, og hvilket lagringsmedie der blev berørt heraf):

10. Antal berørte abonnenter eller fysiske personer

11. Potentielle konsekvenser og potentielle krænkelser af abonnenter eller fysiske personer

12. Tekniske og organisatoriske foranstaltninger, som udbyderen har sat i værk for at afhjælpe potentielle krænkelser

Eventuel yderligere underretning af abonnenter eller fysiske personer

13. Underretningens indhold

14. Anvendte kommunikationsmidler

15. Antal underrettede abonnenter eller fysiske personer

Eventuelle tværnationale spørgsmål

16. Brud på persondatasikkerheden, som involverer abonnenter eller fysiske personer i andre medlemsstater

17. Underretning af andre kompetente nationale myndigheder.

BILAG II

Indholdet af underretningen af abonnenten eller den fysiske person

1. Udbyderens navn

2. Identitet og kontaktoplysninger for den databeskyttelsesansvarlige eller et andet kontaktpunkt, hvor yderligere oplysninger kan indhentes

3. Resumé af hændelsen, der forårsagede bruddet på persondatasikkerheden

4. Datoen, hvor hændelsen skønnes at have fundet sted

5. Karakter og indhold af de berørte personoplysninger, jf. artikel 3, stk. 2

6. Sandsynlige konsekvenser af bruddet på persondatabeskyttelsen for den berørte abonnent eller fysiske person, jf. artikel 3, stk. 2

7. Omstændigheder ved bruddet på persondatasikkerheden, jf. artikel 3, stk. 2

8. Foranstaltninger, som udbyderen har sat i værk for at afhjælpe bruddet på persondatabeskyttelsen

9. Foranstaltninger, som udbyderen anbefaler at sætte i værk for at afbøde eventuelle krænkelser.