



Svensk författningssamling

Brottsdataförordning

Utfärdad den 20 juni 2018

SFS 2018:1202

Publicerad
den 27 juni 2018

Regeringen föreskriver¹ följande.

1 kap. Allmänna bestämmelser

1 § I denna förordning finns kompletterande föreskrifter om sådan behandling av personuppgifter som omfattas av brottsdatalagen (2018:1177).

2 § Uttryck som används i denna förordning har samma innebörd och tillämpningsområde som i brottsdatalagen (2018:1177).

2 kap. Behandling av personuppgifter

1 § Om det visar sig att sådana personuppgifter som anges i 2 kap. 15 § första stycket eller 16 § första stycket brottsdatalagen (2018:1177) har lämnats ut, ska mottagaren omedelbart underrättas om det. Om sådana personuppgifter har gjorts tillgängliga ska, så långt det är möjligt, även den som har tagit del av personuppgifterna omedelbart underrättas.

2 § Den personuppgiftsansvarige ska se till att det finns rutiner för

1. att säkerställa att de som behandlar personuppgifter respekterar tidsfristerna för när personuppgifter inte längre får behandlas, och
2. årlig översyn av behovet av att lagra personuppgifter.

3 § Den som lämnar ut personuppgifter ska underrätta mottagaren om sådana särskilda villkor för behandlingen som har ställts upp med stöd av en bindande EU-rättsakt, en lag eller en förordning.

3 kap. Personuppgiftsansvarigas skyldigheter

Tekniska och organisatoriska åtgärder

1 § De tekniska och organisatoriska åtgärder som den personuppgiftsansvarige ska vidta enligt 3 kap. 2 och 3 §§ brottsdatalagen (2018:1177) ska vara rimliga med hänsyn till behandlingens art, omfattning, sammanhang och ändamål och de särskilda riskerna med behandlingen. När den personuppgiftsansvarige vidtar åtgärder enligt 3 kap. 3 § samma lag ska även de tekniska möjligheterna och kostnaderna för åtgärderna beaktas.

¹ Jfr Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF, i den ursprungliga lydelsen.

Interna strategier

2 § De tekniska och organisatoriska åtgärder som avses i 3 kap. 2 § brottsdatalogen (2018:1117) ska innefatta antagande och dokumentation av interna strategier för dataskydd, om det inte är uppenbart obehövt med hänsyn till verksamhetens begränsade omfattning.

Förteckning över behandlingar

3 § Den personuppgiftsansvarige ska föra en förteckning över de kategorier av behandlingar av personuppgifter som denne ansvarar för. Förteckningen ska innehålla namnet på och kontaktuppgifter till den personuppgiftsansvarige, gemensamt personuppgiftsansvariga och dataskyddsombud. Förteckningen ska dessutom, för varje kategori av behandling, innehålla följande uppgifter:

1. den rättsliga grunden för behandlingen,
2. ändamålen med behandlingen,
3. de kategorier av tjänstemän som har tillgång till de personuppgifter som behandlas,
4. de kategorier av mottagare som uppgifterna kan komma att lämnas ut till, även i tredjeland eller internationella organisationer,
5. de kategorier av registrerade som berörs av behandlingen,
6. de kategorier av personuppgifter som kan komma att behandlas,
7. samlingar av överföringar av personuppgifter till tredjeland eller internationella organisationer,
8. användning av profilering,
9. om det är möjligt, tidsfrister för hur länge kategorierna av personuppgifter får behandlas, och
10. om det är möjligt, en allmän beskrivning av vilka säkerhetsåtgärder som har vidtagits.

Loggning

4 § Skyldigheten att föra loggar i automatiserade behandlingssystem enligt 3 kap. 5 § brottsdatalogen (2018:1177) ska omfatta behandlingar som innebär insamling, ändring, läsning, utlämning, överföring till tredjeland eller internationella organisationer, sammanföring och radering av personuppgifter. Loggarna över läsning och utlämning ska visa datum och tidpunkt för behandlingen och, så långt det är möjligt, vem som har läst eller lämnat ut personuppgifterna och vem som har fått ta del av personuppgifterna.

Tillgången till personuppgifter

5 § Vid tilldelning av behörighet för åtkomst till personuppgifter ska, utöver behovet av uppgifterna, utbildning och erfarenhet särskilt beaktas.

6 § I en behörig myndighet ska det finnas rutiner för tilldelning, förändring, borttagning och regelbunden uppföljning av behörigheter för åtkomst till personuppgifter.

7 § Tillgången till uppgifter om tidigare brottsmisstankar ska särskilt begränsas.

8 § Konsekvensbedömningar som avses i 3 kap. 7 § första stycket brottsdatalogen (2018:1177) ska dokumenteras och innehålla följande uppgifter:

1. en allmän beskrivning av den planerade behandlingen,
2. en bedömning av riskerna för intrång i registrerades personliga integritet,
3. vilka åtgärder som planeras för att hantera riskerna,
4. åtgärder och rutiner för att säkerställa skyddet av personuppgifterna, och
5. rutiner för att visa att tillämpliga dataskyddsregler följs.

9 § Vid förhandssamråd enligt 3 kap. 7 § andra stycket brottsdatalogen (2018:1177) ska den personuppgiftsansvarige lämna in konsekvensbedömningen till tillsynsmyndigheten och tillhandahålla den övriga information som begärs av myndigheten.

Vid bedömningen av om typen av behandling innebär en sådan risk för intrång i registrerades personliga integritet att förhandssamråd ska äga rum ska ny teknik, nya rutiner eller nya förfaranden särskilt beaktas.

Anmälan av överträdelser

10 § Den personuppgiftsansvarige ska ha interna rutiner för anmälan av överträdelser av bestämmelser om personuppgiftsbehandling som garanterar att anmälarens identitet skyddas.

Säkerheten vid behandling av personuppgifter

Säkerhetsåtgärder

11 § Säkerhetsåtgärder enligt 3 kap. 8 § brottsdatalogen (2018:1177) ska åstadkomma en skyddsnivå som är lämplig med hänsyn till

1. de tekniska möjligheterna,
2. kostnaderna för åtgärderna,
3. behandlingens art, omfattning, sammanhang och ändamål,
4. de särskilda riskerna med behandlingen,
5. om känsliga personuppgifter behandlas, och
6. hur integritetskänsliga övriga personuppgifter som behandlas är.

Personuppgiftsincidenter

12 § En anmälan enligt 3 kap. 9 § första stycket brottsdatalogen (2018:1177) ska innehålla följande information:

1. en beskrivning av personuppgiftsincidenten och när den inträffade,
2. om det är möjligt, kategorier av registrerade och det uppskattade antalet registrerade som berörs samt kategorier av personuppgiftsposter och det uppskattade antalet poster som berörs,
3. sannolika konsekvenser av incidenten,
4. vilka åtgärder som vidtagits eller kommer att vidtas med anledning av incidenten,
5. genomförda eller planerade underrättelser till registrerade, och
6. namnet på och kontaktuppgifter till dataskyddsombud eller annan lämplig kontaktpunkt.

All information enligt första stycket ska lämnas samtidigt om det är möjligt.

Om anmälan görs senare än 72 timmar efter det att personuppgiftsincidenten blev känd för den personuppgiftsansvarige, ska förseningen förklaras.

13 § En underrättelse enligt 3 kap. 10 § första stycket brottsdatalagen (2018:1177) ska innehålla följande uppgifter:

1. en beskrivning av personuppgiftsincidenten och när den inträffade,
2. bedömda konsekvenser för den registrerade,
3. vilka åtgärder som vidtagits eller kommer att vidtas med anledning av personuppgiftsincidenten,
4. åtgärder som den registrerade kan vidta för att begränsa skadan, och
5. kontaktuppgifter till dataskyddsombud eller annan lämplig kontaktpunkt.

14 § Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter. Av dokumentationen ska omständigheterna kring incidenten framgå tillsammans med dess effekter och de åtgärder som vidtagits med anledning av den.

15 § Om en personuppgiftsincident som enligt 3 kap. 9 § brottsdatalagen (2018:1177) ska anmälas till tillsynsmyndigheten rör personuppgifter som kommer från eller har lämnats till en behörig myndighet i en annan medlemsstat, ska sådan information som anges i 12 § första stycket utan onödigt dröjsmål lämnas till den myndigheten.

Dataskyddsombud

16 § Den personuppgiftsansvarige ska säkerställa att dataskyddsombud ges möjlighet att delta i de frågor som rör skyddet av personuppgifter.

Den personuppgiftsansvarige ska se till att dataskyddsombud kan utföra de uppgifter som anges i 3 kap. 14 § brottsdatalagen (2018:1177) genom att tillhandahålla nödvändiga resurser, ge tillgång till dokumentation om behandling av personuppgifter och vid behov medge åtkomst till personuppgifter som behandlas. Den personuppgiftsansvarige ska också se till att dataskyddsombud har den sakkunskap som krävs och att de ges möjlighet att upprätthålla denna.

Personuppgiftsbiträden

Avtalets eller överenskommelsens innehåll

17 § Ett avtal eller en annan överenskommelse enligt 3 kap. 16 § andra stycket brottsdatalagen (2018:1177) ska ange vad behandlingen av personuppgifter ska avse, hur länge behandlingen ska pågå, dess art och ändamål, typen av personuppgifter, kategorier av registrerade och den personuppgiftsansvariges skyldigheter och rättigheter. I avtalet eller överenskommelsen ska det särskilt föreskrivas att personuppgiftsbiträdet ska

1. behandla personuppgifter bara enligt instruktioner från den personuppgiftsansvarige,
2. säkerställa att personer som har tillstånd att behandla personuppgifter antingen har förbundit sig att iaktta regler om tystnadsplikt eller omfattas av lagstadgad tystnadsplikt,
3. hjälpa den personuppgiftsansvarige att säkerställa att bestämmelserna om registrerades rättigheter följs,

4. radera eller återlämna alla personuppgifter till den personuppgiftsansvarige när uppdraget har slutförts och, om inte annat följer av lag eller förordning, radera befintliga kopior,

5. ge den personuppgiftsansvarige tillgång till den information som krävs för att visa att det som sägs i denna paragraf, 18 § och 3 kap. 16–18 §§ brottsdatalagen följs, och

6. respektera de villkor som framgår av denna paragraf, 18 § och 3 kap. 17 § brottsdatalagen när ett annat personuppgiftsbiträde anlitas.

Underbiträden

18 § Om den personuppgiftsansvarige har lämnat ett generellt tillstånd enligt 3 kap. 17 § brottsdatalagen (2018:1177), ska personuppgiftsbiträdet informera den personuppgiftsansvarige innan nya personuppgiftsbiträden anlitas.

Förteckning över behandlingar

19 § Varje personuppgiftsbiträde ska föra en förteckning över kategorier av behandlingar av personuppgifter som utförs för en personuppgiftsansvarigs räkning. Förteckningen ska innehålla namnet på och kontaktuppgifter till personuppgiftsbiträdet och dessutom, för varje kategori av behandling, följande uppgifter:

1. namnet på och kontaktuppgifter till eventuella underbiträden,
2. namnet på och kontaktuppgifter till den personuppgiftsansvarige som personuppgiftsbiträdet agerar för,
3. vilka uppgifter som har överförts och till vem, om överföringar av personuppgifter har gjorts till ett tredjeland eller en internationell organisation, och
4. om det är möjligt, en allmän beskrivning av de säkerhetsåtgärder som har vidtagits.

Underrättelseskyldighet

20 § Ett personuppgiftsbiträde ska utan onödigt dröjsmål underrätta den personuppgiftsansvarige om en personuppgiftsincident.

Övriga skyldigheter

21 § Det som sägs om den personuppgiftsansvariges skyldigheter i 4 och 11 §§ gäller även för personuppgiftsbiträden.

Gemensamt personuppgiftsansvariga

22 § Gemensamt personuppgiftsansvariga ska i en skriftlig överenskommelse reglera sina respektive förpliktelser i egenskap av personuppgiftsansvarig. I överenskommelsen ska det särskilt regleras

1. hur ansvaret för enskildas rättigheter ska utövas och vars och ens skyldighet att tillhandahålla information enligt 4 kap. 1 och 2 §§ brottsdatalagen (2018:1177), och
2. vem som ska vara kontaktpunkt för registrerade.

En sådan överenskommelse som anges i första stycket får inte innebära att de personuppgiftsansvarigas författningenliga skyldigheter inte fullgörs.

Bemyndiganden

23 § Tillsynsmyndigheten får meddela ytterligare föreskrifter om

1. sådana åtgärder som avses i 3 kap. 2–4 och 8 §§ brottsdatalagen (2018:1177),
2. krav och rutiner för loggning enligt 3 kap. 5 § brottsdatalagen,
3. vilka typer av behandlingar som ska omfattas av förhandssamråd enligt 3 kap. 7 § andra stycket brottsdatalagen, och
4. anmälan och underrättelse om personuppgiftsincidenter.

4 kap. Enskildas rättigheter

Krav på utformningen av information

1 § Information enligt 3 kap. 10 § första stycket och 4 kap. 1–4 §§ brottsdatalagen (2018:1177) ska vara lättillgänglig och lättbegriplig och lämnas i lämplig form. Detsamma gäller information enligt 3–7 §§, 3 kap. 13 § och 5 kap. 2 § denna förordning.

Enskilds begäran

2 § En begäran enligt 4 kap. 3, 4, 9 eller 10 § brottsdatalagen (2018:1177) ska göras skriftligen hos den personuppgiftsansvarige.

Den personuppgiftsansvarige ska säkerställa att begäran görs av en behörig person.

Beslut

3 § Beslut enligt 4 kap. 5, 7, 9 och 10 §§ och 12 § andra stycket brottsdatalagen (2018:1177) ska vara skriftliga. Beslut som går den registrerade emot ska motiveras.

Av 4 kap. 5 § andra och tredje styckena brottsdatalagen framgår att skälen för vissa beslut inte behöver lämnas ut.

Underrättelser

Underrättelser till enskilda

4 § Sökanden ska utan onödigt dröjsmål underrättas om beslut enligt 4 kap. 5 § första eller tredje stycket brottsdatalagen (2018:1177) i fråga om information enligt 4 kap. 3 § samma lag. Sökanden ska i sådana fall också underrättas om möjligheterna att lämna in klagomål till tillsynsmyndigheten och begära kontroll enligt 5 kap. 3 § brottsdatalagen. Någon underrättelse behöver inte lämnas om det skulle skada det intresse som föranleder att information inte lämnas.

5 § Sökanden ska underrättas om beslut enligt 4 kap. 7 § första stycket eller 12 § andra stycket brottsdatalagen (2018:1177).

6 § Den registrerade ska underrättas om beslut enligt 4 kap. 9 eller 10 § brottsdatalagen (2018:1177) och om möjligheten att lämna in klagomål till tillsynsmyndigheten. Om den personuppgiftsansvarige med stöd av 4 kap. 5 § andra eller tredje stycket brottsdatalagen inte har lämnat ut skälen för beslutet, ska den registrerade också underrättas om möjligheten att begära kontroll enligt 5 kap. 3 § brottsdatalagen.

7 § Den registrerade ska underrättas innan en begränsning enligt 4 kap. 9 § andra stycket brottsdatalagen (2018:1177) upphör.

8 § Den myndighet från vilken personuppgifter kommer ska underrättas om beslut enligt 4 kap. 9 § första stycket brottsdatalagen (2018:1177).

Den som har tagit emot personuppgifter ska underrättas om beslut enligt 4 kap. 9 eller 10 § brottsdatalagen.

5 kap. Tillsyn

Kontroll genom tillsynsmyndigheten

1 § En begäran enligt 5 kap. 3 § brottsdatalagen (2018:1177) ska göras skriftligen och ange behörig myndighet och mål, ärende, förteckning eller verksamhetsområde som begäran om kontroll gäller.

Tillsynsmyndigheten ska säkerställa att begäran görs av en behörig person.

2 § Tillsynsmyndigheten ska skriftligen underrätta den sökande om att kontroll enligt 5 kap. 3 § brottsdatalagen (2018:1177) har utförts.

Beslut att vägra utföra kontroll ska vara skriftliga och motiveras.

Förhandssamråd

3 § Om tillsynsmyndigheten anser att en sådan planerad behandling som avses i 3 kap. 7 § brottsdatalagen (2018:1177) kan komma att stå i strid med lag eller annan författning, ska myndigheten senast sex veckor efter det att begäran om samråd togs emot skriftligen lämna råd enligt 5 kap. 6 § första stycket samma lag. Om det finns särskilda skäl, får tiden förlängas med en månad. Tillsynsmyndigheten ska inom en månad från det att begäran om samråd togs emot informera om förlängningen och om orsakerna till den.

Samarbete med utländska tillsynsmyndigheter

Utländsk begäran om bistånd

4 § En begäran om bistånd från en tillsynsmyndighet i en annan medlemsstat ska besvaras så snabbt som möjligt och senast en månad efter det att begäran togs emot. Den som begärt bistånd ska underrättas om handläggningen och om resultatet av begäran.

5 § Om bistånd till en tillsynsmyndighet i en annan stat vägras, ska den som begärt biståndet underrättas. I underrättelsen ska skälen för vägran anges.

Svensk begäran om bistånd av en annan medlemsstat

6 § Tillsynsmyndigheten får begära bistånd av en tillsynsmyndighet i en annan medlemsstat med sådana åtgärder som myndigheten får vidta när den utövar tillsyn.

7 § En begäran om bistånd ska innehålla all information som behövs för att tillsynsmyndigheten i den andra medlemsstaten ska kunna besvara begäran. Syftet med och skälen för åtgärden ska anges.

Internationella överenskommelser

8 § Tillsynsmyndigheten får, trots det som sägs i 9 §, ingå överenskommelser med tillsynsmyndigheter i andra medlemsstater om avgifter för internationellt bistånd.

9 § Tillsynsmyndigheten ska utföra sina tillsynsuppgifter avgiftsfritt, om inte något annat bestäms.

6 kap. Administrativa sanktionsavgifter

1 § Sanktionsavgifter ska betalas till Kammarkollegiet.

2 § En beslutad sanktionsavgift faller bort till den del beslutet om avgiften inte har verkställts inom fem år från det att beslutet fick laga kraft.

3 § Om betalningsansvaret har upphävts genom ett beslut som fått laga kraft, ska sanktionsavgiften betalas tillbaka. För en sanktionsavgift som betalas tillbaka betalas även ränta enligt 5 § räntelagen (1975:635) för tiden från den dag då avgiften betalades till och med den dag den betalas tillbaka.

7 kap. Överföring av personuppgifter till tredjeland och internationella organisationer

1 § Den som har överfört personuppgifter till ett tredjeland eller en internationell organisation utan ett förhandsmedgivande enligt 8 kap. 2 § andra stycket brottsdatalagen (2018:1177) ska utan dröjsmål informera den medlemsstat som lämnat uppgifterna till en svensk myndighet om överföringen.

2 § Om en svensk myndighet har överfört personuppgifter enligt 8 kap. 8 § brottsdatalagen (2018:1177), ska myndigheten utan onödigt dröjsmål informera behörig myndighet i det tredjelandet om överföringen. Det som nu har sagts gäller inte om det skulle vara ineffektivt eller olämpligt att informera om överföringen.

3 § Överföringar av personuppgifter enligt 8 kap. 4 § 2 och 5 § brottsdatalagen (2018:1177) ska dokumenteras. Av dokumentationen ska det framgå vilka personuppgifter som överförts, datum och tidpunkt för överföringen, ändamålet med och grunden för överföringen och till vilken myndighet som personuppgifterna överfördes.

På begäran ska dokumentationen göras tillgänglig för tillsynsmyndigheten.

4 § Den personuppgiftsansvarige ska informera tillsynsmyndigheten om samlingar av överföringar som görs enligt 8 kap. 4 § 2 brottsdatalagen (2018:1177).

5 § Överföringar av personuppgifter enligt 8 kap. 8 § brottsdatalagen (2018:1177) ska dokumenteras. Den personuppgiftsansvarige ska informera tillsynsmyndigheten om sådana överföringar.

1. Denna förordning träder i kraft den 1 augusti 2018.

2. Genom förordningen upphävs förordningen (2013:343) med vissa bestämmelser om skydd för personuppgifter vid polissamarbete och straffrättsligt samarbete inom Europeiska unionen.

3. Bestämmelsen i 3 kap. 4 § om loggning tillämpas från och med den 6 maj 2023 i fråga om automatiserade behandlingssystem som inrättats före den 6 maj 2016.

På regeringens vägnar

SFS 2018:1202

MORGAN JOHANSSON

Ida Wettervik
(Justitiedepartementet)