Avdelningen för verksamhetsstöd och -styrning
Sofia Palmér
Avsändarens e-postadress

Personuppgiftspolicy

Denna personuppgiftspolicy är en avsiktsförklaring och riktlinje för att styra beslut och hjälpa medarbetare på IVO att efterleva dataskyddsförordningen.

Policyn beskriver på ett övergripande plan hur IVO samlar in, lagrar och använder personuppgifter.

IVO är som organisation personuppgiftsansvarig för all behandling av personuppgifter som myndigheten utför. I förekommande fall kan personuppgiftsbiträde anlitas för behandling.

IVO har antagit denna personuppgiftspolicy för behandling av personuppgifter i syfte att säkerställa att samtliga inom organisationen har information om och därmed följer tillämplig dataskyddslagstiftning.

Innehåll

1. Behandling av personuppgifter

All behandling av personuppgifter på IVO ska ske i enlighet med gällande dataskydds-bestämmelser.

Gällande dataskyddsbestämmelser omfattar bland annat dataskyddsförordningen[1], kallad GDPR, vilken gäller som lag i Sverige, samt nationella kompletterande bestämmelser[2] till förordningen.

IVO:s anställda och uppdragstagare får endast behandla personuppgifter enligt de styrdokument för personuppgiftsbehandling som IVO tagit fram i form av policy, riktlinje, rutin eller i annan instruktion.

1.1. Begrepp och definitioner

Begrepp och definitioner som används i personuppgiftspolicyn har samma betydelse som i dataskyddsförordningen.[3]

1.2. Laglighet, korrekthet och öppenhet

Varje behandling ska vara laglig och i enlighet med principerna i dataskydds-förordningen.[4]

Behandling av personuppgifter på IVO måste vara nödvändig för att IVO ska kunna utföra sina uppgifter. Alla behandlingar ska ske på ett öppet sätt i förhållande till den registrerade.[5]

1.3. Ändamålsbegränsning

Om IVO överväger att behandla personuppgifterna för andra ändamål än det ändamål för vilket personuppgifterna samlades in, måste det senare påkomna ändamålet vara förenligt med det ursprungliga.

Syftet med behandlingen ska fastställas innan behandling sker av uppgifterna och kan inte anges i efterhand. Däremot hindrar förordningen inte att personuppgifter bevaras för arkivändamål även om de ursprungligen samlades in för ett annat ändamål.[6] Se under 1.5.

---

[1] Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning).
[2] T.ex. dataskyddslagen (2018:18)
[3] Artikel 4 dataskyddsförordningen
[4] Artikel 5 och 6 dataskyddsförordningen.
[5] Artikel 5.1 dataskyddsförordningen. Undantag kan förekomma om sekretess föreligger gentemot den registrerade i enlighet med offentlighets- och sekretesslagen (2009:400),OSL
[6] Se prop. 2017/18:105 s. 109

1.4. Uppgiftsminimering

Alla personuppgifter som behandlas ska vara adekvata, relevanta och begränsade till vad som är nödvändigt för de ändamål som de behandlas för.

De ändamål som personuppgifterna behandlas för ska vara tydligt formulerade.

1.5. Lagringsminimering

Personuppgifterna får inte förvaras i en form som möjliggör identifiering av den registrerade under längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

IVO är dock skyldig att bevara sina allmänna handlingar enligt arkivlagen[7]. Det innebär att personuppgifter kan behöva bevaras även om de ursprungligen samlades in och behandlades för ett annat ändamål än arkivändamål av allmänt intresse. Sådan ytterligare behandling för arkivändamål är enligt de grundläggande principerna inte oförenlig med de ursprungliga ändamålen.

1.6. Integritet och konfidentialitet

Personuppgifter som IVO behandlar ska hanteras och förvaras så att obehöriga inte får tillgång till dem.

2. Samtycke

IVO ska inom myndighetens uppdrag normalt inte behandla personuppgifter med stöd av samtycke.

Myndigheter kan som huvudregeln inte åberopa samtycke som rättslig grund för att behandla personuppgifter eftersom det råder betydande ojämlikhet mellan den registrerade och den personuppgiftsansvarige.[8]

Innan en behandling sker med stöd av samtycke måste det noga utredas och dokumenteras att samtycket bedömts kunna lämnas frivilligt och utgöra en giltig rättslig grund för behandlingen. Om bedömning görs att samtycke är en giltig rättslig grund ska samtycke som huvudregel lämnas skriftligt och på ett sådant sätt att det tydligt går att särskilja från övrig text och information. Det ska vidare framgå vad den registrerade samtycker till och rätten att när som helst återkalla samtycket.

3. Behandling av särskilda kategorier av personuppgifter

Vissa personuppgifter är till sin natur mer känsliga än andra. I dataskyddsförordningen anses följande kategorier av personuppgifter kräva ett särskilt skydd:

[7] Arkivlagen (1990:782)
[8] Skäl 43 dataskyddsförordningen

- ras eller etniskt ursprung,
- politiska åsikter,
- religiös eller filosofisk övertygelse,
- medlemskap i en fackförening,
- hälsa,
- en persons sexualliv eller sexuella läggning och
- genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.

Huvudregeln är att känsliga personuppgifter inte får behandlas, men IVO får behandla känsliga personuppgifter i följande fall med stöd i dataskyddslagen.

3.1. När det krävs enligt lag

IVO får behandla känsliga personuppgifter om uppgifterna har lämnats till IVO och behandlingen krävs enligt lag[9]. Det här undantaget innebär att IVO får behandla känsliga personuppgifter bland annat när det är nödvändigt för att hantera allmänna handlingar, till exempel när myndigheten tar emot e-post.

3.2. För att kunna handlägga ärenden

IVO får också behandla känsliga personuppgifter om det är nödvändigt för handläggningen av ett ärende. [10]

3.3. I andra fall

IVO kan även i annat fall behöva behandla känsliga personuppgifter. Detta är tillåtet om behandlingen är nödvändig med hänsyn till ett viktigt allmänt intresse och den inte innebär ett otillbörligt intrång i den registrerades personliga integritet. [11]

3.4. Om behandlingen är nödvändig för arkivändamål av allmänt intresse.

Behandling av känsliga personuppgifter är tillåten för arkivändamål om behandlingen är nödvändig för att den personuppgiftsansvarige ska kunna följa föreskrifter om arkiv. [12]

4. Kontakt med registrerade

All kontakt med de registrerade ska ske på ett klart, tydligt och lättillgängligt språk. För att underlätta för enskilda att ta tillvara sina rättigheter ska IVO ha en tydlig kontaktväg gällande frågor avseende dess behandlingar av personuppgifter.

---

[9] 3 kap. 3 § 1 dataskyddslagen.
[10] 3 kap. 3 § 2 dataskyddslagen.
[11] 3 kap. 3 § 3 dataskyddslagen.
[12] 3 kap. 6 § dataskyddslagen.

När IVO samlar in personuppgifter om den registrerade, direkt från den registrerade själv eller från någon annan källa, ska den registrerade informeras om behandlingen och de rättigheter som de registrerade har enligt gällande dataskyddsbestämmelser.[13]

IVO behöver inte informera den registrerade om behandlingen om det visar sig vara omöjligt eller detta skulle medföra en oproportionell ansträngning.[14] Det gäller även om uppgifter har samlats in från någon annan än den registrerade. Det är då viktigt att sådana bedömningar dokumenteras.

4.1. Personer med sekretessmarkerade folkbokföringsuppgifter

Vid kommunikation med och om personer med sekretessmarkerade personuppgifter ska endast säkra kommunikationskanaler användas. Säkra kommunikationskanaler är brev[15], elektronisk kommunikation som skyddas med kryptering och autentisering av mottagaren med hjälp av elektronisk legitimation samt besök av den enskilde om han eller hon har legitimerat sig.

För utskick till en person med sekretessmarkerade personuppgifter gäller särskild hantering.[16]

5. Begäran om tillgång

Enskilda personer har rätt att förhöra sig om IVO behandlar deras personuppgifter. IVO ska vid begäran från den registrerade lämna bekräftelse på om personuppgifterna som rör den registrerade behandlas samt lämna tillgång till personuppgifterna och den information som krävs enligt dataskyddsförordningen (registerutdrag).

Lämpliga och rimliga identifikationsåtgärder ska vidtas för att säkerställa att informationen lämnas till rätt person.[17]

6. Hantering

En inkommen begäran om information, tillgång till personuppgifter, radering, rättelse, begränsning av behandling eller invändning mot behandling av personuppgifter ska hanteras utan onödigt dröjsmål.

6.1. Begäran om rättelse och registrering

En begäran om rättelse och radering av personuppgifter ska hanteras i enlighet med författningskrav. Om en felaktig personuppgift har registrerats ska alla rimliga åtgärder vidtas för att uppgiften rättas eller raderas och det ska ske utan onödigt dröjsmål.[18]

---

[13] Artikel 13-18 och 20-21 i dataskyddsförordningen.
[14] Artikel 14.5 dataskyddsförordningen.
[15] Med brev avses här postbefordran med mottagningskvitto.
[16] Se s. 80 i rutinen ”Hantera handlingar”, dnr. 1.3–6784/2018
[17] Artikel 15 i dataskyddsförordningen
[18] Artikel 16-17 i dataskyddsförordningen

Detta påverkas dock av om personuppgiften finns i en allmän handling eller inte. En till IVO inkommen handling blir en allmän handling och ska registreras eller hållas ordnad. Enligt arkivlagen är myndigheter skyldiga att bevara allmänna handlingar oförändrade.

6.2. E-post

E-post innebär i princip alltid behandling av personuppgifter. Själva e-postadressen i sig är oftast en personuppgift och all annan information i meddelandet som kan kopplas till en enskild person är också personuppgifter.

Den personuppgiftsbehandling som sker i e-post ska därför uppfylla alla de krav som finns i dataskyddsförordningen. IVO måste göra samma bedömningar för behandlingen av personuppgifter i e-post som för behandlingen av personuppgifter i andra system. Det innebär bland annat att det måste finnas en rättslig grund som tillåter att IVO behandlar personuppgifterna.

Det som skiljer e-post från annan uppgiftshantering är att innehållet oftast är okänt när e-posten kommer in. Utgångspunkten är att IVO behöver ta hand om inkommande post och kan stödja det på att det är en uppgift av allmänt intresse och en rättslig skyldighet.

7. Personuppgiftsansvar

IVO är som organisation personuppgiftsansvarig och bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Det är alltså inte någon enskild individ som är personuppgiftsansvarig.

Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med dataskyddsförordningen. Dessa åtgärder ska ses över och uppdateras vid behov.

Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Om extern part får i uppdrag att behandla personuppgifter för IVO:s räkning ska ett personuppgiftsbiträdesavtal ingås. Av avtalet ska de instruktioner som IVO lämnar till biträdet tydligt framgå. Den personuppgiftsansvarige är alltid ansvarig för ingående av personuppgiftsbiträdesavtal.

Ett personuppgiftsbiträde får endast anlitas om biträdet kan lämna tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska säkerhetsåtgärder för att därigenom kunna säkerställa att den registrerades rättigheter skyddas.

IVO:s mall för personuppgiftsbiträdesavtal ska i princip alltid användas. Avtal ska följas upp vid behov och minst en gång per år. Uppföljningen ska framförallt ske för att kontrollera att biträdena följer biträdesavtalet och de instruktioner som IVO har lämnat för behandlingen, men även andra kontroller kan göras för att säkerställa att gällande lagstiftning följs.

8. Registerförteckning

Det ska enligt dataskyddsförordningen finnas ett register över de behandlingar av personuppgifter som IVO utför under sitt ansvar.[19]

IVO:s register[20] innehåller information om lagstadgade uppgifter och hålls uppdaterat av dataskyddsombudet. Registret innehåller också uppgifter om ändamålen med behandlingen, kategorier av registrerade, personuppgifter samt mottagare.

Registret ska uppvisas i samband med tillsyn från tillsynsmyndigheten.

9. Säkerhet

Personuppgifterna ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna. Vid behandling av personuppgifter ska lämpliga organisatoriska och tekniska säkerhetsåtgärder vidtas för att förhindra obehörig eller otillåten åtkomst eller annan behandling samt för att skydda personuppgifter mot förlust, förvanskning eller skada genom till exempel otillåtna handlingar eller olyckshändelser.

Vid val av lämpliga säkerhetsåtgärder ska behandlingens art, känsligheten av personuppgifterna, ändamålet, sammanhanget och omfattningen av behandlingen beaktas. Vidare ska eventuella risker bedömas och kostnader samt tekniska möjligheter beaktas.

9.1. Personuppgiftsincidenter

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks.

Med personuppgiftsincident avses en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,

Alla uppkomna personuppgiftsincidenter måste anmälas till tillsynsmyndigheten (Datainspektionen) inom 72 timmar efter det att överträdelsen har upptäckts. Anmälan gör

[19] Skäl 82 i dataskyddsförordningen.
[20] Excellista ”GDPR förteckning PuA och PuB (Register)”.

det möjligt för Datainspektionen att bland annat bevaka vad IVO gör för att motverka negativa effekter.

Detta ansvar gäller även i de fall som IVO anlitar ett personuppgiftsbiträde och det inträffar en personuppgiftsincident hos dem, då måste personuppgiftsbiträdet omedelbart rapportera det till IVO.

10. Dataskyddsombud

På IVO finns ett dataskyddsombud som har till uppgift att informera och ge råd om skyldigheter enligt gällande dataskyddsbestämmelser samt övervaka efterlevnaden av dessa.

Dataskyddsombudet ger på begäran råd gällande konsekvensbedömning avseende dataskydd och övervakar genomförandet av den.

IVO:s dataskyddsombud fungerar även som kontaktpunkt för tillsynsmyndigheten (Datainspektionen) i frågor som rör personuppgiftsbehandling, inbegripet det förhandssamråd som skall genomföras, med tillsynsmyndigheten, om en konsekvensbedömning visar att personuppgiftsbehandlingen leder till en hög risk om inte IVO vidtar åtgärder för att minska risken.

11. Ändringar i personuppgiftspolicyn

IVO kan komma att komplettera och ändra denna personuppgiftspolicy.

Ändringar kan framförallt vara påkallade som en följd av förändringar i gällande rätt.

Denna personuppgiftspolicy kan kompletteras av riktlinjer som är mer specifika för vissa delar av IVO:s uppdrag. När ändringar görs i denna policy, kommer det att framgå av revisionsdatumet längst ned på denna sida. Den ändrade personuppgiftspolicyn är gällande efter det datumet.

11.1. Ikraftträdande

Denna policy har antagits vid GD-föredragning den 19 december 2018.

Ändring	Datum