Göteborgs Stad
Försäkrings AB Göta Lejon

Tjänsteutlåtande

2018-06-12

Diarienummer:

Handläggare: Katrin Kajrud

Tel: 031-368 55 12
E-post: katrin.kajrud@gotalejon.goteborg.se

Punkt 16 Policy och riktlinje för hantering av personuppgifter i Försäkrings AB Göta Lejon

Förslag till beslut i styrelsen för Försäkrings AB Göta Lejon

- att anta policy och riktlinje för hantering av personuppgifter i Försäkrings AB Göta Lejon

Bakgrund

Efter beslut i staden behövs ingen policy och riktlinje eftersom man anser det vara lag.

För Försäkrings AB Göta Lejon finns dock ett krav att som bolag inneha en policy och riktlinje för hantering av personuppgifter.

Bilagor

1. Policy och riktlinje för hantering av personuppgifter i Försäkrings AB Göta Lejon

- Bilaga 1 Instruktion för hantering av registrerads persons begäran om rättning eller borttagande av personuppgift

- Bilaga 2 Instruktion för hantering av risker avseende personuppgiftshantering i ostrukturerat material

- Bilaga 3 Instruktion för hantering av Privacy by design

Katrin Kajrud	Annika Forsgren
Bolagsjurist	VD

Göteborgs Stad
Försäkrings AB Göta Lejon

FÖRSÄKRINGS AB GÖTA LEJON	Policy och riktlinje för hantering av personuppgifter i Försäkrings AB Göta Lejon		Rättslig grund GDPR - dataskyddsförordningen
Dokumentnamn	**Antagen datum**	**Löpnummer**	**Version**
Policy och riktlinje för hantering av personuppgifter i Försäkrings AB Göta Lejon	2018-06-12	B680A000XX	Version: 1
Dokumenttyp	**Publiceras**	**Dokumentansvarig**	**Operativt ansvarig**
Policy och riktlinje	Intranätet	Styrelsen	Bolagsjurist

Policy för hantering av personuppgifter i Försäkrings AB Göta Lejon

Varje behandling av personuppgifter ska ske med hänsyn till den enskildes personliga integritet och rättigheter.

Varje behandling av personuppgifter ska ske i enlighet med gällande lagstiftning

Vid behandling av personuppgifter ska följande grundläggande principer tillämpas:

- Behandlingen ska vara laglig, korrekt och öppen gentemot den registrerade
- Ändamålsbegränsning - Innan behandling påbörjas ska ett särskilt och uttryckligt samt berättigat ändamål med behandlingen vara fastställt. Hantering utöver detta ändamål kan vara otillåtet då det kan vara oförenligt med det ursprungliga ändamålet
- Insamling av uppgifter - Endast de uppgifter som är adekvata och relevanta för ändamålet får samlas in. Insamlingen får inte vara mer omfattande än nödvändigt - Insamlade personuppgifter ska vara korrekta och uppdaterade.
- Lagringsminimering - Insamlade personuppgifter får bara bevaras i identifierbar form så länge det är nödvändigt för ändamålet
- Åtkomstbegränsning – endast behöriga ska få åtkomst till personuppgifter
- Integritet och konfidentialitet – Lämpliga tekniska och organisatoriska åtgärder baserade på informationssäkerhetsklassningar och riskanalyser ska skydda personuppgifterna
- Ansvar - Den personuppgiftsansvarige ska kunna visa att behandlingen sker med följsamhet till principerna
- Försäkrings AB Göta Lejon ska vara representerat av ett dataskyddsombud
- Vid varje behandling av personuppgifter ska ett sådant förhållningssätt iakttas att risken för skada för den registrerade minimeras.

Riktlinje för hantering av personuppgifter i Försäkrings AB Göta Lejon

Inledning

Följande riktlinje syftar till att konkretisera policyn samt ge vägledning och råd vid hantering av personuppgifter i Försäkrings AB Göta Lejon.

Riktlinjen, som grundar sig på bestämmelserna i lagstiftningen och kan komma att justeras vid förändringar av gällande rätt.

Omfattning

Denna riktlinje gäller för Försäkrings AB Göta Lejon. Riktlinjen avser hantering av personuppgifter som helt eller delvis företas på automatisk väg samt på annan än automatisk behandling av personuppgifter som ingår eller kommer att ingå i ett register. Med ett register avses en strukturerad samling uppgifter som är tillgängliga för sökning eller sammanställda enligt särskilda kriterier.

Bakgrund

Från och med den 25 maj 2018 gäller EU:s dataskyddsförordning (679/2016) för hantering av personuppgifter. Förordningen ersätter personuppgiftslagen, PuL (1998:204). Förordningen behöver inte implementeras i svensk rätt genom svensk lag utan är direkt tillämplig.
Genom den nya lagstiftningen ska den tillit som behövs för att utveckla den digitala ekonomin över hela den inre marknaden uppnås. Det är av stor vikt att fysiska personer har kontroll över sina egna personuppgifter. Målet med dataskyddsförordningen anges vara att stärka och harmonisera den rättsliga säkerheten och smidigheten för fysiska personer, ekonomiska operatörer och myndigheter i unionen.

Övergångsregler

All pågående behandling ska vara anpassad till förordningen den 25 maj 2018. Om pågående behandling grundar sig på samtycke enligt direktiv 95/46/EG, är

det inte nödvändigt att den registrerade på nytt ger sitt samtycke för att den personuppgiftsansvarige ska kunna fortsätta med behandlingen i fråga efter det att denna förordning börjar tillämpas, om det sätt på vilket samtycket gavs överensstämmer med villkoren i denna förordning. Beslut av kommissionen som antagits och tillstånd från tillsynsmyndigheterna som utfärdats på grundval av direktiv 95/46/EG ska fortsatt vara giltiga tills de ändras, ersätts eller upphävs.

Materiellt tillämpningsområde

Förordningen ska tillämpas på all hantering av personuppgifter som helt eller delvis företas på automatisk väg samt på annan än automatisk behandling av personuppgifter som ingår eller kommer att ingå i ett register.

Personuppgiftsansvar

Försäkrings AB Göta Lejon är personuppgiftsansvariga för sitt verksamhetsområde. Ansvaret innebär en yttersta skyldighet att tillse att gällande lagstiftning efterlevs genom att bl.a.

- Fastställa ändamål och syfte med behandling av personuppgifter, innan behandling påbörjas
- Utse dataskyddsombud och svara för att denne har förutsättningar och besitter erforderlig kunskap och för att fullgöra sitt uppdrag
- Säkerställa att det finns tekniska och organisatoriska förutsättningar att behandla personuppgifter med erforderlig säkerhet
- Kunna visa att kraven i lagstiftningen är uppfyllda genom noggrann dokumentation samt verifierande tester
- Föra register över behandlingar av personuppgifter

Laglig behandling av personuppgifter

Personuppgifter får endast behandlas om det finns laglig grund för behandlingen. Den lagliga grunden ska fastställas innan behandling påbörjas enligt någon av nedan punkter:

- Samtycke – ska vara informerat, frivilligt och specifikt samt kunna visas.
- Behandlingen är nödvändig för att fullgöra ett avtal

- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som den personuppgiftsansvarige har
- Behandlingen är nödvändig för att skydda ett grundläggande intresse för den registrerade eller annan fysisk person
- Behandlingen är nödvändig för att utföra uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning.

Innan behandling av personuppgifter påbörjas krävs följande:

1. Dokumentera ändamål och syfte samt under hur lång tid behandlingen beräknas pågå
2. Fastställ rättslig grund
3. Inhämta samtycke vid behov
4. Säkerställ att behandlingen sker i enlighet med de grundläggande principerna och denna policy och riktlinje
5. Vid behov, rådgör med dataskyddsombudet
6. Klassificera personuppgifterna utifrån informationssäkerhetsnivå och genomför en riskanalys av den planerade behandlingen. Dataskyddsombudet ska involveras i riskanalysen.
7. Samråd med tillsynsmyndighet om hög risk inte kan åtgärdas inför behandling av personuppgifter
8. Se till att det finns tillräckliga tekniska och organisatoriska säkerhetsåtgärder utifrån genomförd informationssäkerhetsklassning och resultat från riskanalys
9. Klargör om, och i så fall vilken, kommunikation med den registrerade som är nödvändigt
10. Upprätta personuppgiftsbiträdesavtal vid behov
11. Se till att dataskyddsombudet godkänner behandlingen
12. Anteckna ny behandling av personuppgifter i PuL-databasen

Säkerhet

Behandling av personuppgifter får ske om lämplig teknisk och organisatorisk säkerhet vidtagits för behandlingen. Säkerheten ska baseras på genomförda informationssäkerhetsklassningar och riskanalyser.
Säkerhet utgörs av:

Inbyggt dataskydd och dataskydd som standard vilket för personuppgiftshanteringen bl.a. innebär:

- att säkerställandet av personuppgiftshanteringen ska finnas med redan från den initiala planeringen och täcka såväl tekniska som organisatoriska åtgärder
- säkerställa att stadens grundsäkerhetsnivå för informationssäkerhet (nivå 1) föreligger samt om möjligt nyttja åtgärder som pseudonymisering, anonymisering eller kryptering
- säkerställa att stadens förhöjda säkerhetsnivå (nivå 2) för informationssäkerhet föreligger avseende särskilda personuppgifters konfidentialitet och riktighet vilket för elektronisk hantering bl a innebär nyttjande av kryptering samt stark autentisering motsvarande tillitsnivå 3 för e-legitimation
- nyttja åtgärder som uppgiftsminimering, lagringsminimering, fritextfältsmimimering och åtkomstbegränsning

Införande och tillämpning av rutiner för att:

- Kontinuerligt testa, undersöka och visa på effektiviteten av införda säkerhetsåtgärder
- Anmäla personuppgiftsincident till tillsynsmyndighet
- Vid behov kunna ge incidentinformation till berörda registrerade
- Vid behov kunna involvera och rådgöra med dataskyddsombudet

Personuppgiftsbiträde

Den som behandlar personuppgifter på uppdrag av annan personuppgiftsansvarig blir personuppgiftsbiträde i förhållande till den personuppgiftsansvarige. Vid anlitandet av ett personuppgiftsbiträde ska säkerställas att denne kan ge tillräckliga garantier om att upprätthålla lämplig teknisk och organisatorisk säkerhet i enlighet med gällande rätt.

Personuppgiftsbiträdesavtal

Personuppgiftsbiträdets (biträdet) behandling av personuppgifter ska regleras av personuppgiftsbiträdesavtal mellan biträdet och den personuppgiftsansvarige (ansvarige). I avtalet ska anges:

- Vem som är personuppgiftsansvarig respektive personuppgiftsbiträde.

- Vad behandlingen avser, dess varaktighet, art, ändamål, typ av personuppgifter samt kategori av registrerade

- Den ansvariges skyldigheter och rättigheter

- Att biträdet endast får behandla personuppgifter i enlighet med den ansvariges instruktion

- Att biträdet iakttar erforderlig konfidentialitet och tystnadsplikt

- Att biträdet vidtar alla lämpliga tekniska och organisatoriska åtgärder för att säkerställa adekvat skydd för personuppgifterna samt att detta kan visas genom att ge ansvarige tillgång till vederbörlig information

- Att biträdet ska bistå den ansvarige i att uppfylla sina förpliktelser enligt förordningen.

- Att biträdet inte får anlita underleverantör för behandling av den ansvariges personuppgifter utan den ansvariges skriftliga medgivande till detta. Om biträdet anlitar underleverantör ska personuppgiftsbiträdesavtal upprättas även mellan dessa parter.

- Att överföring till tredje land inte får ske utan att adekvata säkerhetsåtgärder är uppfyllda.

- Reglering om inom vilken tid radering eller överflyttning av personuppgifter sker vid avtals upphörande.

Register över behandling

Varje personuppgiftsansvarig ska föra ett register över behandling som utförs under dess ansvar. Registret ska minst innehålla:

- Namn och kontaktuppgifter till den personuppgiftsansvarige samt dataskyddsombudet
- Ändamålet med behandlingen
- Kategori av registrerade, personuppgifter samt behandlingar
- Mottagare av personuppgifter, i förekommande fall
- Eventuell överföring till tredje land med tillhörande säkerhetsåtgärder

  Uppskattad tidsfrist för radering
- Beskrivning av tekniska och organisatoriska säkerhetsåtgärder för behandlingen om inte detta hindras av exempelvis sekretessbestämmelser

Dataskyddsombud

Den personuppgiftsansvarige ska utse ett dataskyddsombud att representera den ansvariges verksamhet. Det kan vara en person för flera verksamheter och det kan vara en anställd eller extern konsult. Dataskyddsombudet ska utses på grundval av sina yrkesmässiga kvalifikationer och i synnerhet sakkunskap om lagstiftning och praxis avseende dataskydd. Dataskyddsombudet ska anmälas till tillsynsmyndigheten. Dataskyddsombudet ska minst ha följande uppgifter:

- Informera och ge råd till den personuppgiftsansvarige och anställda om skyldigheterna enligt dataskyddsförordningen
- Övervaka efterlevnad av förordningen avseende fungerande rutiner och åtgärder, ansvarstilldelning, information, utbildning och granskning
- Ge råd vid riskanalysen
- Samarbeta med tillsynsmyndigheten
- Vara kontaktpunkt för tillsynsmyndigheten i alla frågor som rör behandling av personuppgifter
- Vara kontaktperson till den registrerade
- Delta i frågor som rör skyddet av personuppgifter
- Får även ha andra uppgifter om det inte leder till intressekonflikt

Den personuppgiftsansvarige ska säkerställa att dataskyddsombudet:

- På ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter
- Tillhandahålla de resurser och det stöd som krävs för att fullgöra sina uppgifter
- Upprätthålla ombudets sakkunskap
- Inte blir föremål för sanktioner eller avsätts på grund av att ombudet utför sitt uppdrag
- Inte bli föremål för otillbörlig påverkan i utövande av sitt uppdrag
- Rapporterar direkt till den personuppgiftsansvarige eller dennes högsta förvaltningsnivå

Göteborgs Stad
Försäkrings AB Göta Lejon

FÖRSÄKRINGS AB GÖTA LEJON	Instruktion för hantering av registrerad persons begäran om rättning eller borttagning av personuppgifter		**Rättslig grund** **GDPR**
Dokumentnamn	**Antagen datum**	**Löpnummer**	**Version**
Instruktion för hantering av registrerad persons begäran om rättning eller borttagning av personuppgifter	2018-06-12	B680A000XX	Version: 1
Dokumenttyp	**Publiceras**	**Dokumentansvarig**	**Operativt ansvarig**
Instruktion	Intranätet	VD	Bolagsjurist

Instruktion för hantering av registrerad persons begäran om rättning eller borttagning av personuppgifter

Syfte:

En individ (en registrerad person) har en lagstadgad rätt att begära rättning eller borttagning av sina personuppgifter.

Denna instruktion har till syfte att beskriva hur en begäran om rättning eller borttagning av personuppgifter ska hanteras på FÖRETAGET. Genom en gemensam instruktion för hantering kan FÖRETAGET upprätthålla en enhetlig och effektiv behandling av sådana förfrågningar.

Instruktionen riktar sig till samtliga medarbetare inom FÖRETAGET med specifikt fokus på de roller vilka kan komma i kontakt med begäran om rättning eller borttagning av personuppgifter.

Upplägg:
Denna instruktion är upplagd som en steg-för-steg-instruktion där svaret på respektive fråga hänvisar dig vidare till nästa steg. Om det vid ett steg anges att ingen ytterligare aktivitet krävs behöver efterföljande frågeställningar inte besvaras.

Utförande roller:
Följande roller är primära utförare:

- Dataskyddsombud
- Registeransvarig

Stödjande dokument:
Dokumentation från genomgång av denna instruktion sker i följande bilagor:

- *Bilaga A - Svarsbrev 1*
- *Bilaga B - Svarsbrev 2*

I instruktionen står vilken eller vilka bilagor som blir relevanta för den aktuella situationen.

Instruktion:

1. Dataskyddsombudet tar emot begäran och kontrollerar följande:
   a) Innehåller begäran uppgifter om vilken registrerad person som begär åtgärden?

b) Kan det med tillräcklig säkerhet säkerställas att det är den registrerade personen själv som ligger bakom begäran?

Nästa steg	
Om svaret är ja på samtliga frågor	Gå vidare till fråga 2.
Om svaret är nej på fråga a)	Dataskyddsombudet informerar den registrerade om vilken komplettering som krävs för att kunna avgöra vilken registrerad person som begär åtgärden. Uppdatera samtliga adresser i dokumentet när ny hänvisning är beslutat. Alternativt hänvisa även till e-postadress då även förfrågningar som inkommer via e-post kan uppfylla kraven. När efterfrågad komplettering har inkommit, gå vidare till fråga 2.
Om svaret är nej på fråga b)	Dataskyddsombudet informerar den registrerade om vilken komplettering som krävs alt. på vilket sätt begäran behöver lämnas för att kunna avgöra vilken registrerad person som begär åtgärden. Uppdatera samtliga adresser i dokumentet när ny hänvisning är beslutat. Alternativt hänvisa även till e-postadress då även förfrågningar som inkommer via e-post kan uppfylla kraven. *Exempel på metoder för identifiering:* - *Är begäran inkommen skriftligen och undertecknad?* - *Är begäran inkommen i inloggat läge?* - *Har den registrerade personens identitet fastställts genom kopia på den registrerades ID-handling? (Kommentar: Kopian på ID-handlingen måste sedan förstöras när kontrollen av denna är klar och dokumenterad på lämpligt ställe.)* - *Har den registrerade personens identitet fastställts i enlighet med eventuell instruktion för identifiering på distans, exempelvis genom kundnummer (som endast den rätta personen kan antas ha åtkomst till) eller genom kontrollfrågor?)* När det med tillräcklig säkerhet kunnat säkerställas att det är den registrerade personen själv som ligger bakom begäran, gå vidare till

	fråga 2. ***Notera**: Om förutsättningar saknas för att med tillräcklig säkerhet säkerställa att det är den registrerade som ligger bakom begäran, kan som alternativ metod övervägas att som kontrollmetod skicka uppmaning om komplettering till den registrerades folkbokföringsadress. Det rekommenderas dock att upprätta en rutin för identifiering, exempelvis enligt identifieringsmetoderna ovan.*

2. Dataskyddsombudet besvarar följande frågeställning:
   a) Innehåller begäran uppgifter om vilken åtgärd som begärs?

Nästa steg	
Om svaret är ja	Gå vidare till fråga 3.
Om svaret är nej	Dataskyddsombudet informerar den registrerade om att begäran ska innehålla information om vilken åtgärd begäran gäller, som exempelvis uppdatering av felaktiga kontaktuppgifter, borttagning av kontaktuppgifter insamlade för marknadsföringsändamål eller borttagning av samtliga kontaktuppgifter (”rätten att bli glömd”). När efterfrågad komplettering inkommit, gå vidare till fråga 3.

3. Dataskyddsombudet besvarar följande frågeställning (och rådgör vid behov med berörd registeransvarig):
   a) Kan den begärda rättningen/borttagningen genomföras i FÖRETAGETs system med ett bestående resultat?

Kommentar: Om uppgifterna läses in från en extern part (exempelvis folkbokföringsregistret) där FÖRETAGET inte kan uppdatera uppgifterna behöver den registrerade kontakta den externa parten för att rättningen eller borttagningen ska bli bestående.

Nästa steg	
Om svaret är ja	Gå vidare till fråga 4.
Om svaret är nej	Informera den registrerade om att dennes uppgift blivit rättad/borttagen, men att uppgiften inom kort kommer läsas in igen från det aktuella externa registret, och att begäran om åtgärd därför

	även bör göras hos den externa part vilken uppgifterna hämtas ifrån. Om begäran gäller flera åtgärder gå sedan vidare till fråga 4, annars krävs ingen ytterligare aktivitet.

4. Dataskyddsombudet besvarar följande frågeställningar:
   a) Gäller begäran rättning av felaktiga personuppgifter?
   b) Gäller begäran borttagning av samtliga personuppgifter för den registrerade (den så kallade rätten att bli glömd) alternativt borttagning av specifika personuppgifter?

Nästa steg	
Om svaret är ja på a)	Gå vidare till fråga 5
Om svaret är ja på b)	Gå vidare till fråga 6
Om svaret är ja på både a) och b)	Gå vidare till fråga 5 och följ stegen fram tills att ingen vidare åtgärd krävs, gå därefter vidare till fråga 6.

5. Dataskyddsombudet besvarar följande frågeställning:
   a) Finns det något skäl till att en rättning av de aktuella uppgifterna inte bör ske?

   Kommentar: Ett exempel är att den postadress den registrerade vill ändra till inte existerar. Beroende på vilken uppgift det rör sig om kan det vara nödvändigt att verifiera att den ändring som begärs överensstämmer med verkliga förhållanden. Särskild vaksamhet krävs om den begärda ändringen skulle kunna ha till avsikt att på ett bedrägligt sätt vinna fördelar för den registrerade.

Nästa steg	
Om svaret är ja	Dataskyddsombudet informerar den registrerade om varför en rättning av personuppgifterna inte kan genomföras genom att fylla i: • Bilaga B - Svarsbrev 2 Dataskyddsombudet skickar ovan information till den registrerades folkbokföringsadress.

	Ingen ytterligare aktivitet krävs därefter.
Om svaret är nej	Dataskyddsombudet: • Informerar aktuell registeransvarig om vilka uppgifter som ska rättas. Registeransvarig: • Utför rättningen, och • Bekräftar till dataskyddsombudet när rättningen är genomförd. Dataskyddsombudet: • Fyller i svarsbrev enligt *Bilaga A -Svarsbrev 1* Dataskyddsombudet skickar följande information till den registrerades folkbokföringsadress: • *Bilaga A -Svarsbrev 1* Ingen ytterligare aktivitet krävs därefter.

6. Dataskyddsombudet kontrollerar i FÖRETAGETs förteckning över behandling av person-uppgifter (i normalfallet registerförteckningen) vilka personuppgifter FÖRETAGET har avseende den registrerade personen och besvarar om någon av nedanstående förutsättningar är för handen.

   Notera: Om radering har begärts av fler än en personuppgift, ska förutsättningarna nedan kontrolleras för varje separat typ av personuppgift som omfattas av begäran. Exempelvis kan vissa uppgifter fortfarande vara ”nödvändiga” i den mening som avses i punkt a) nedan, medan andra uppgifter inte längre är det.

   a) Är personuppgifterna inte längre nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats?
   b) Har den registrerade återkallat ett samtycke på vilket behandlingen grundat sig och det finns inte någon annan rättslig grund för behandlingen?

c) Har den registrerade invänt mot behandlingen i enlighet med artikel 21.1 och det saknas berättigade skäl för behandlingen som väger tyngre, eller har den registrerade invänt mot behandlingen i enlighet med artikel 21.2?
d) Har personuppgifterna behandlats på olagligt sätt?
e) Måste personuppgifterna raderas för att uppfylla en rättslig förpliktelse enligt EU-rätten eller nationell rätt?
f) Har personuppgifterna samlats in i samband med erbjudande av informationssamhällets tjänster direkt till en omyndig? (Se GDPR artikel 8.1.)

Kommentar: Se även instruktion för gallringsrutiner för exempel på lagar som kan kräva att uppgifter sparas.

Nästa steg	
Om svaret är att någon av förutsättningarna ovan är uppfylld (besvaras per behandling)	Grundläggande förutsättningar för radering föreligger (för den aktuella behandlingen). Specialregler kan dock förhindra radering. Gå vidare till fråga 7.
Om svaret är att ingen av förutsättningarna ovan är uppfylld (besvaras per behandling)	FÖRETAGET kan inte tillgodose den registrerades begäran för den aktuella behandlingen, i fråga om den aktuella personuppgiften. Dataskyddsombudet: • Sammanställer vilka typer av uppgifter FÖRETAGET inte kan ta bort. När samtliga behandlingar är hanterade, gå vidare till fråga 8.

7. Dataskyddsombudet kontrollerar i FÖRETAGETs förteckning över behandling av personuppgifter och besvarar följande frågeställning:

   Behöver FÖRETAGET fortsätta behandla personuppgifterna för:

   a) Att utöva rätten till yttrande- och informationsfrihet?

b) Att annan lag förhindrar att de relevanta personuppgifterna kopplade till den registrerade inte kan raderas av FÖRETAGET?
c) Skäl som rör ett viktigt allmänt intresse på folkhälsoområdet enligt artikel 9.2 h och artikel 9.3.
d) Arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål enligt artikel 89.1, då borttagning av personuppgifterna omöjliggör eller avsevärt försvårar uppnåendet av syftet med den behandlingen?
e) Behöver FÖRETAGET fortsätta behandla personuppgifterna för att fastställa, göra gällande eller försvara rättsliga anspråk?

Kommentar: Det som främst bör kunna bli aktuellt i FÖRETAGETs fall är b) eller e). Exempel på detta är då man för en anställd på FÖRETAGET behöver behålla uppgifter om den registrerades inkomst för att kunna rapportera detta till Skatteverket; därför kan relevanta uppgifter för detta inte tas bort (alternativ b)). Ett annat exempel då behov av att spara personuppgifter kan finnas är då FÖRETAGET har skickat en faktura till den registrerade som inte är betalad (alternativ e)).

Se även instruktion för gallringsrutiner för exempel på lagar som kan kräva att uppgifter sparas.

Nästa steg	
Om svaret är ja (besvaras per behandling)	FÖRETAGET kan inte tillgodose den registrerades begäran för den aktuella behandlingen. Dataskyddsombudet: • Sammanställer vilka typer av uppgifter FÖRETAGET inte kan ta bort. När samtliga behandlingar är hanterade, gå vidare till fråga 8.
Om svaret är nej (besvaras per behandling)	FÖRETAGET kan tillgodose den registrerades begäran för den aktuella behandlingen. Dataskyddsombudet skickar följande till berörd registeransvarig: • Information om vilka personuppgifter som ska tas bort.

	Registeransvarig: • Utför rättningen, och • Bekräftar till dataskyddsombudet när borttagningen är genomförd. När samtliga behandlingar är hanterade, gå vidare till fråga 8

8. Besvara följande frågeställning:
   a) Har den registrerades begäran om borttagning av personuppgifter kunnat tillgodoses?

      *Kommentar: Så är fallet för aktuell behandling om 1) någon av förutsättningarna i fråga 6 ovan är uppfylld **och** 2) svaret är nej på fråga 7.*

Nästa steg	
Om svaret är ja	Dataskyddsombudet: • Fyller i svarsbrev enligt *Bilaga A -Svarsbrev 1* och informerar där om att borttagning av de aktuella personuppgifterna kunnat ske. Dataskyddsombudet skickar följande information till den registrerades folkbokföringsadress alt. genom säkert meddelande exempelvis i inloggat läge: • *Bilaga A -Svarsbrev 1* Ingen ytterligare aktivitet krävs därefter.
Om svaret är nej	Dataskyddsombudet: • Fyller i svarsbrev enligt *Bilaga B -Svarsbrev 2* och informerar där om att borttagning av de personuppgifter (vissa eller samtliga) inte kunnat ske samt vilka typer av personuppgifter som berörs. Dataskyddsombudet skickar följande information till den registrerades folkbokföringsadress alt. genom säkert meddelande exempelvis i inloggat läge: • *Bilaga B -Svarsbrev 2*

	Ingen ytterligare aktivitet krävs därefter.

Bilaga A - Svarsbrev 1

Hej XXXXX, Datum: ÅÅMMDD

Du har begärt rättning/borttagning av dina personuppgifter som FÖRETAGET behandlar. FÖRETAGET bekräftar att rättningen/borttagningen är genomförd.

Med vänlig hälsning,

XXXXXXX

Som registrerad har du rätt att begära rättelse eller radering av personuppgifterna som rör dig. Du har också rätt att begära begränsning av behandlingen av dina personuppgifter eller invända mot sådan behandling. Du har även rätt att inge klagomål till en tillsynsmyndighet.

För frågor kring Försäkring AB Göta Lejon behandling av personuppgifter, vänligen kontakta oss via brev till adress: Försäkrings AB Göta Lejon, Stora Badhusgatan 6, 411 21 Göteborg

---

Bilaga B - Svarsbrev 2

Hej XXXXX, Datum: ÅÅMMDD

Du har begärt rättning/borttagning av dina personuppgifter som FÖRETAGET behandlar. FÖRETAGET bekräftar att rättningen/borttagningen är genomförd men att följande typ av uppgifter inte kunnat rättas/tas bort:

X - På grund av XXX
X - På grund av XXX
X - På grund av XXX

Med vänlig hälsning,

XXXXXXX

Som registrerad har du rätt att begära rättelse eller radering av personuppgifterna som rör dig. Du har också rätt att begära begränsning av behandlingen av dina personuppgifter eller invända mot sådan behandling. Du har även rätt att inge klagomål till en tillsynsmyndighet.

För frågor kring Försäkring AB Göta Lejon behandling av personuppgifter, vänligen kontakta oss via brev till adress: Försäkrings AB Göta Lejon, Stora Badhusgatan 6, 411 21 Göteborg

---

Göteborgs Stad
Försäkrings AB Göta Lejon

FÖRSÄKRINGS AB GÖTA LEJON	**Instruktion för hantering av risker avseende personuppgiftshantering i ostrukturerat material**		**Rättslig grund** **GDPR**
Dokumentnamn	**Antagen datum**	**Löpnummer**	**Version**
Instruktion för hantering av risker avseende personuppgiftshantering i ostrukturerat material	2018-06-12	B680A000XX	Version: 1
Dokumenttyp	**Publiceras**	**Dokumentansvarig**	**Operativt ansvarig**
Instruktion	Intranätet	VD	Bolagsjurist

Instruktion för hantering av risker avseende personuppgiftshantering i ostrukturerat material

Syfte:
En av viktigaste ändringarna som EU:s dataskyddsförordning medför för svensk del är att den s.k. ”missbruksregeln” för behandling av personuppgifter i ostrukturerat material försvinner. Detta innebär att all typ av behandling av personuppgifter måste uppfylla samma krav, oavsett om behandlingen sker i strukturerade databaser/arkiv eller i s.k. ostrukturerat material, dvs. i löpande text, e-post, video etc.

Denna instruktion har till syfte att beskriva hur riskerna kan inventeras och minskas i fråga om hantering av personuppgifter i ostrukturerat material. Instruktionen riktar sig i första hand till dataskyddsombudet samt till chefer och linjechefer inom organisationen, som ansvarar för att en eller flera delar av organisationen lever upp till dataskyddsförordningens krav (samt övriga relaterade regler, inklusive rekommendationer från tillsynsmyndigheten (Datainspektionen/Integritetsskydds-myndigheten). [Instruktioner som i stället riktar sig till medarbetare i deras dagliga hantering av personuppgifter finns i form av dokumentet Instruktion för medarbetares hantering av personuppgifter i ostrukturerat material.]

Arbetet med att utifrån detta dokument inventera och hantera riskerna med behandlingen i ostrukturerat material är inte att betrakta som en engångsinsats. Det är i stället en fråga som bör tas upp med regelbundenhet eftersom både arbetssätt och tekniska och organisatoriska förutsättningar tenderar att vara i ständig förändring.

Genom en gemensam instruktion för hantering kan detta ske på likvärdiga grunder och garantera att organisationen uppfyller de krav som dataskyddsförordningen för med sig för ostrukturerat material.

Instruktionens utformning:
Denna instruktion är indelad i två delar. Del 1 behandlar inventering, kategorisering och riskbedömning av hantering i ostrukturerat material. Den är upplagd som en steg för steg-instruktion där svaret på respektive fråga hänvisar vidare till nästa steg. Om det vid ett steg anges att ingen ytterligare aktivitet krävs behöver efterföljande frågeställningar inte besvaras.

Del 2 fokuserar på hur organisationen kan vidta lämpliga åtgärder och skapa ändamålsenliga rutiner. Dataskyddslagstiftningen föreskriver inte i detalj vilka åtgärder som ska vidtas.

Lagstiftningen anger i stället som huvudregel att lämpliga åtgärder ska vidtas utifrån integritetsriskerna med behandlingen. Valet av åtgärder måste med andra ord göras utifrån ett riskbaserat synsätt med hänsyn tagen till de aktuella omständigheterna. Instruktionens del 2 behöver läsas med de ögonen och betraktas som en vägledning och rekommendation, eftersom något facit inte går att fastställa.

Utförande roller:
Följande roller är primära utförare:

- Dataskyddsombud
- Linjechef

Del 1 – Inventering och riskbedömning

1) **Förekommer hantering av personuppgifter i ostrukturerat material?**

   Kommentar: Hantering av personuppgifter i ostrukturerat material är all hantering som inte sker inom ramen för sökbara register (både digitala och pappersregister).

   Exempel på hantering i ostrukturerat material är exempelvis:
   E-post (extern och intern)
   Chat och forum
   Arbetsdokument på gemensamma lagringsytor (inkl. excel-filer)
   I löpande text (t.ex. i en artikel eller ett word-dokument)
   Videoupptagning
   Ljudupptagning
   Enklare listor och minnesanteckningar
   Sparade dokument på skrivbordet

   Uppgifter av rent privat karaktär täcks i normalfallet inte av dataskyddsförordningens regler.

   Notera: Angående e-post är även avsändaradresser, namn, e-postsignaturer etc som förekommer i e-postmeddelanden också att betrakta som personuppgifter. <u>För riskbedömningen och valet av säkerhetsåtgärder nedan ska dock påpekas att sådana uppgifter normalt sett har en låg grad av integritetskänslighet.</u>

   Datainspektionens rekommendationer är att man bör informera varje person som skickar e-post till organisationen om hur man hanterar deras personuppgifter. Som exempel nämner Datainspektionen information genom ett svar eller ett autosvar där

man länkar till en integritetspolicy på sin webbplats, eller redan i kontaktformuläret om man använder ett sådant.

Datainspektionen rekommenderar även att personer som omnämns i e-post kan behöva informeras om att man behandlar personuppgifter som rör henne eller honom. Man får göra en sammanvägd bedömning utifrån omständigheterna i varje enskilt fall om arbetsinsatsen för att få tag i personen och ge informationen står i proportion till vikten av att personen informeras. Om det rör sig om personuppgifter av okänslig karaktär, exempelvis i sedvanlig e-postkorrespondens mellan kollegor eller i andra vardagliga meddelanden, anser Datainspektionen att det normalt sett är oproportionerligt att kräva att den tredje personen informeras särskilt.

Nästa steg	
Om svaret är ja	Gå vidare till steg 2.
Om svaret är nej	Ingen ytterligare aktivitet krävs.

2) Finns god medvetenhet om hur hanteringen av personuppgifter i ostrukturerat material sker i dagsläget samt vilka krav som ställs av dataskyddsregelverket?

Kommentar: Generellt finns i många organisationer idag låg medvetenhet om den hantering av personuppgifter som finns i ostrukturerat material samt de risker som är förknippade med detta, då många har använt sig av den så kallade ”missbruksregeln”.

När missbruksregeln försvinner innebär det att samma regler som gäller för personuppgifter i databaser och system, också ska användas för personuppgifter i ostrukturerat material.
Det innebär bl.a. att följande krav behöver uppfyllas:

- *Laglig grund*
- *Grundläggande principer för behandling*
- *Informationsklassning av personuppgifter*
- *Fungerande gallringsrutiner*
- *Inkludera behandlingarna i registerförteckningen*
- *Rutiner för styrning och kontroll*

Nästa steg

Om svaret är ja	En god medvetenhet om den aktuella hanteringen i ostrukturerat material underlättar arbetet med att få kontroll över hanteringen. Det underlättar även utförande av uppgifterna under punkten 6 nedan. (Mindre fokus behöver läggas på punkt 3, 4 och 5.)
Om svaret är nej	Detta är som ovan nämnt utgångsläget för många organisationer i utgångsläget. Fråga 3, 4 och 5 bör ges lämpligt utrymme, **där dock den största insatsen bör läggas på åtgärderna som föreslås under punkt 6**.

3) Har organisationen inventerat sin hantering av personuppgifter i ostrukturerat material?

Nästa steg	
Om svaret är ja	Utvärdera om inventeringen behöver kompletteras, och gå sedan vidare till fråga 4)
Om svaret är nej	Kartlägg i vilka sammanhang/system/processer som personuppgifter behandlas i ostrukturerat material. Kartlägg vilka typer/kategorier av personuppgifter som finns i ostrukturerat material (se exempel under punkt 1 ovan). Kategoriseringen kan anpassas utifrån verksamhetens inriktning, men för att utgöra ett lämpligt stöd för riskbedömning måste varje sådan kategorisering identifiera integritetskänsliga typer av personuppgifter. Exempel på sådana kategorier är: - ”Särskilda kategorier” (se dataskyddsförordningen artikel 9) - Brottsuppgifter - Uppgifter om person med skyddad identitet - Integritetskänsliga personuppgifter

	Kartlägg vidare följande: - Vilket ändamål har behandlingen? - Är behandlingen nödvändig med hänsyn till ändamålet? - Vilken laglig grund har behandlingen? - Delas uppgifterna till extern part? (I så fall vilken?) Dokumentera koncist men ändamålsenligt. Gå sedan vidare till fråga 4. Angående dokumentering: Man bör lägga störst fokus på hur man vill att en framtida hantering ska se ut, inte att dokumentera varenda detalj kring en existerande process som man ändå vill modifiera eller rent av eliminera.

4) Identifiera och utvärdera riskerna med behandlingen.

Nästa steg
Utvärdera om några av uppgifterna/behandlingarna behöver mer skydd/särskild behandling (som särskilda kategorier av eller integritetskänsliga personuppgifter) än andra och gå sedan vidare till fråga 5. Exempel på faktorer som påverkar riskerna: - Uppgifternas känslighet ur ett integritetsperspektiv - Hur stor volym av uppgifter det rör sig om (i synnerhet känsliga uppgifter) - Hur stor krets som har tillgång till uppgifterna - I vilken utsträckning uppgifterna delas (i synnerhet externt men även internt) - Vilken spridning uppgifterna skulle kunna få

Tänk exempelvis på:

- Uppgifter som rör individer i egenskap av privatpersoner normalt sett ses som känsligare än i yrkesrollen.
- Uppgifter som hanteras digitalt (särskilt i e-post) lättare kan få stor spridning jämfört med uppgifter som hanteras manuellt

Dokumentera koncist men ändamålsenligt. När riskanalysen är klar, gå vidare till del 2 för att identifiera vilka åtgärder som kan genomföras för att minska riskerna.

Del 2 – Risksänkande åtgärder

I fråga om risksänkande åtgärder finns en mängd olika åtgärder som kommer att presenteras nedan.

Som inledning kan följande principer nämnas som målsättningar för att minska riskerna med hantering av personuppgifter i ostrukturerat material:

- **Minimera hanteringen av personuppgifter i e-post**: E-post kan lätt hackas och dessutom kan det lätt få stor spridning. Dela hellre dokument och känsliga uppgifter med hjälp av gemensamma filytor eller använd krypterad överföring.
- **Styr hanteringen mot förvaltade system**: I system finns många tekniska säkerhetsåtgärder som kan vidtas (kryptering, automatisk gallring, behörighetsstyrning m.m.) som inte är tillgängliga på samma sätt vid hantering som är manuell eller på annat sätt sker utanför system.
- **Utbilda!** Se till att personalen har kunskap och ett integritetsmedvetet sätt att se på sina arbetsuppgifter. Då kan personalen fatta kloka beslut i sin vardagliga hantering av personuppgifter och även hjälpa organisationen att identifiera integritetsrisker i det dagliga arbetet.

1) **Rensning och minimering**

   Ett första naturligt steg är att minimera mängden uppgifter som behandlas på ett riskfyllt sätt. Detta gäller naturligtvis särskilt för de känsliga uppgifterna.

Nästa steg

Baserat på inventeringen så finns det följande huvudalternativ för åtgärder:

- Radera de uppgifter som inte är tillåtna (saknar laglig grund) eller inte längre är nödvändiga för det ändamål för vilket de samlades in. Nödvändigt innebär att det ska finnas ett konkret och rimligt skäl. ”Kan vara bra att ha” är inte skäl nog.
- Flytta personuppgifter i ostrukturerat material till förvaltade system
- Flytta personuppgifter som är integritetskänsliga, känsliga, rör skyddad identitet eller brottsuppgifter till mapp med strikt behörighetsåtkomst (bör ses som tillfällig lösning)

Ett ytterligare sätt att minimera mängden uppgifter är även att styra vilka uppgifter som kommer in till organisationen, så att endast de uppgifter som verkligen är nödvändiga behöver behandlas. Exempel:

- Ta kontakt med företagskunder, leverantörer, partners etc. om det förekommer onödiga uppgifter i fakturor, lönespecifikationer (personnummer är ett vanligt exempel) och andra liknande dokument. Detsamma kan gälla arbetssätt per e-post.
- Se på motsvarande sätt över organisationens blanketter och liknande så att de uppgifter som begärs faktiskt är nödvändiga för ändamålet med personuppgiftsbehandlingen.
- För kontaktvägar till den egna organisationen är det ofta att rekommendera att kommunikationen hänvisas till webbformulär hellre än e-post. I ett formulär kan man styra vilka uppgifter som får läggas in (och man kan även slippa att få in bifogade filer, om det skulle vara ett problem).
- Stäng av funktioner för automatisk lagring av historik i exempelvis chatt-applikationer (Skype for Business och extern chatt).

2) Informationsklassning

Nästa steg
Om organisationen använder sig av ett informationsklassningssystem: Påbörja informationsklassning av de personuppgiftsbehandlingar som ska behållas. Det rekommenderas starkt att låta personuppgiftsbehandlingen bli en naturlig del av organisationens informationsklassningsmodell.

3) Säkerhetsåtgärder

Nästa steg
Med utgångspunkt i den riskanalys som beskrivits ovan i del 1, analysera vilka säkerhetsåtgärder som vore lämpliga för att komma tillrätta med de identifierade riskerna. Exempel på relevanta kontrollfrågor (många ja är ett tecken på att starka säkerhetsåtgärder krävs): - Behandlas personuppgifter om många personer? - Behandlas en stor mängd personuppgifter om varje person? - Finns det risk för att personuppgifterna kan spridas på ett oönskat sätt? - Är det svårt att kontrollera att behandling endast sker i enlighet med ändamålen med behandlingen? - Kan många användare komma åt personuppgifterna? - Hanteras personuppgifter via öppna nät som internet, t.ex. webbhemsida eller e-post? - Hur stor är sannolikheten för och konsekvenserna av tekniska störningar? - Hur stor är sannolikheten för och konsekvenserna av att obehöriga får åtkomst till uppgifterna?

4) Se över arbetssätt

Utifrån vad som sagts ovan om framför allt inventering, riskanalys och minimering – se över och ifrågasätt existerande arbetssätt utifrån ett integritetsperspektiv. Tänk särskilt på att HR-avdelningen i de allra flesta organisationer ofta hanterar mycket personliga och känsliga uppgifter.

Nästa steg
Exempel på konkreta råd för att förbättra säkerheten i organisationens hantering av personuppgifter: - **E-posta personuppgifter så sällan som möjligt**. Minimera kommunikation av personuppgifter per e-post, både externt och internt. E-post skapar digitala spår och kan hackas och det digitala formatet medför att det snabbt kan få mycket stor spridning. E-post innebär dessutom alltid en spridningsrisk pga. felaktiga e-postadresser,

vidarebefordrande eller namnförväxlingar etc. Kan man ta för vana att kommunicera uppgiften muntligt till kollegan i stället? Kan uppgiften skrivas ner på ett papper som sedan kastas så snart det går?

- **Använd gemensamma filytor**. Sträva alltid mot att dela uppgifter med hjälp av gemensamma filytor eller kommunikationsytor (både internt och externt) i stället för att e-posta. Kommunikationen blir i regel betydligt säkrare än via e-post.

- **Spara på bara ett enda ställe**. Undvika att flera exemplar (och versioner!) av dokument cirkulerar i organisationen. Minska spridningsrisken genom att exempelvis spara på en gemensam filyta. Om gemensamma e-postinkorgar används: Använd av samma skäl inte automatisk vidarebefordring till de behöriga personernas egna inkorgar. Låt i stället en notifiering skickas till de egna inkorgarna.

- **Använd krypteringslösningar**. Organisationen bör tillhandahålla en funktionell krypteringslösning för de fall där personuppgifter måste delas per e-post. (Beroende på krypteringslösning kan det vara viktigt att det finns en lättillgänglig och lättbegriplig instruktion till hands för medarbetarna.)

- **Skapa inbox-regler**. Känslig e-post ska inte ligga kvar i inkorgen. Det som inte kan raderas omedelbart ska sorteras in i mappar (som med fördel kan namnges på ett sätt som signalerar att det är konfidentiellt material). Detta av flera skäl:

    1) Det minskar risken för att någon får se uppgifterna av misstag

    2) En särskild mapp som signalerar att det rör sig om konfidentiellt material skapar en höjd mental tröskel för någon att obehörigen gå in och titta på uppgifterna.

    3) Det ger möjlighet att använda automatiska gallringsfrister för inkorgen

    4) Det ger kontroll över vilka känsliga meddelanden som finns i mapparna, så att de kan gallras manuellt eller med automatiska gallringsfrister.

- **Ansvar**: Utse ansvariga personer, så som informationsägare/mappägare till gemensamma filytor och ansvariga för gemensamma inkorgar.

- **Kodlås på skrivare**. Utskrifter som innehåller personuppgifter ska inte

komma under någon annans ögon. Skrivare som kräver att en personlig kod knappas in är att anses som ett måste för att leva upp till dataförordningens krav.

5) Gallringsrutiner

En fungerande regelbunden gallring är helt central för att kunna leva upp till dataskyddsförordningens krav. Enligt huvudregeln får en personuppgift bara sparas så länge den är *nödvändig* för det ändamål för vilket den samlades in.

Nästa steg

Checklista för att skapa förutsättningar för en fungerande gallring:

- **Automatisk gallring**: Detta är alltid att rekommendera så långt det är möjligt och gäller inte bara förvaltade system utan alla tänkbara applikationer såsom inkorgar och mappar i Outlook, filytor, m.m. Att spara personuppgifter (då i särskilda mappar el. likn.) ska vara ett *aktivt val*.
- **Manuell gallringsrutin**: Om sådan krävs – se till att det finns dokumentation över rutinen. Följ upp att det blir gjort med rätt regelbundenhet.
- **Gallringstabell**: Säkerställ att det finns en ändamålsenlig tabell över gallringsfrister som gäller för verksamheten.
- **Utbilda och medvetandegör**: Se till att vikten av en fungerande gallring är känd i organisationen. Se till att gallringstabell och gallringsrutiner är kända och finns lättillgängliga.

Göteborgs Stad
Försäkrings AB Göta Lejon

FÖRSÄKRINGS AB GÖTA LEJON	Instruktion för hantering av Privacy by design		Rättslig grund GDPR
Dokumentnamn	**Antagen datum**	**Löpnummer**	**Version**
Instruktion för hantering av privacy by design	2018-06-12	B680A000XX	Version: 1
Dokumenttyp	**Publiceras**	**Dokumentansvarig**	**Operativt ansvarig**
Instruktion	Intranätet	VD	Bolagsjurist

Instruktion för Privacy by design

Syfte:

Denna instruktion har till syfte att beskriva hur Privacy by Design (s.k. inbyggt integritetsskydd) ska tas i beaktande vid utveckling, konfigurering, inköp, förvaltning och avveckling av system/processer. FÖRETAGET har ansvar för att vid behandling av personuppgifter alltid ha individens integritet i fokus. Som grundläggande principer inom integritetsskydd kan i det här sammanhanget särskilt nämnas:

- att inte samla in mer information än vad som behövs,
- att inte ha informationen kvar längre än man behöver och
- att inte använda informationen till något annat än vad man samlade in den för.

Genom att utforma IT-system med eftertanke kan man skapa en integritetsmedveten och integritetssäker hantering från början till slut. Detta är grundtanken bakom Privacy by Design. Generellt ska varje organisation som behandlar personuppgifter kunna påvisa att personuppgifter i standardfallet behandlas i enlighet med de principer som gäller enligt dataskyddslagstiftningen. Genom en gemensam instruktion för att beakta principerna om inbyggt dataskydd och dataskydd som standard ökar förmågan att leva upp till kraven enligt dataskyddslagstiftningen.

Det är av stor vikt att dessa frågor utgör en naturlig del av FÖRETAGETs processer för utveckling, förändring och inköp av system eller processer.

Utförande roller:

Följande roller är primära utförare:

- Dataskyddsombud
- IT-säkerhetsansvarig
- Informationssäkerhetsansvarig
- Beställare/inköpare
- Registeransvarig

Principer för Privacy by Design

Rubrikerna nedan i denna instruktion utgörs av de sju principer för Privacy by Design som anses allmänt vedertagna på global nivå.

Dataskyddsförordningen slår fast att lämpliga åtgärder ska vidtas med hänsyn till riskerna med personuppgiftsbehandlingen i fråga. Det innebär att ett riskbaserat synsätt ska anläggas i fråga om utformning och konfigurering av de system som hanterar personuppgifter. Alla typer av åtgärder kommer därför inte att vara nödvändiga för alla system. Denna instruktion ska ses som en rekommendation för hur bästa möjliga integritetsskydd kan byggas in i IT-system. I fråga om system som hanterar känslig information bör de allra flesta åtgärderna nedan vara aktuella. Det anges särskilt nedan vilka åtgärder som bör anses obligatoriska.

1. **Var proaktiv och förhindrande i stället för reaktiv och korrigerande**

I de fall där personuppgiftsbehandlingen kan leda till en hög risk för fysiska personers rättigheter och friheter kräver GDPR att en konsekvensanalys ska utföras, en s.k. PIA (Privacy Impact Assessment). Den innehåller en kartläggning av konsekvenserna för integriteten hos de som är registrerade i systemet. Syftet med en PIA är att identifiera och bedöma risker med personuppgiftsbehandlingen samt att analysera vilka åtgärder som kan vidtas för att minska riskerna till en acceptabel nivå.

2. **Gör integritet till standardinställning (Privacy by default)**

Privacy by default innebär att systeminställningarna är inställda på ett sätt som ger största möjliga integritetsvänlighet. I de fall där det finns olika alternativ ska standardinställningarna vara inställda på de alternativ som ger bästa integritetsskydd. Till exempel ska det på en sociala webbplats vara standard att profilen och personuppgifterna är dolda och att det är användaren själv som aktivt måste välja vad som ska visas.

3. **Integritet inbäddad i designen**

Med detta avses att systemet enbart ska samla/hämta och behandla de personuppgifter som är nödvändiga. Genom rätt åtgärder och funktionalitet kan man låta systemet styra användaren mot ett integritets-säkert arbetssätt. Nedan anges exempel på olika sätt att begränsa mängden personlig information och hur informationen behandlas till vad som är nödvändigt.

Följande åtgärder bör betraktas som *obligatoriska* för så gott som alla system som behandlar personuppgifter:

- Behörigheten i systemet begränsas till enbart de roller eller grupper som behöver ha åtkomst. Systemet tillåter endast att användare får tillgång till den information som krävs för att utföra sin specifika uppgift. När en användare söker information som skiljer sig från rollens definierade behov, finns det rutiner så att användaren måste dokumentera sitt behov av utökad åtkomst.
- Användargränssnittet begränsar möjligheten att registrera och i övrigt behandla onödig personlig information. Det finns enbart fält för uppgifter som är nödvändiga för ändamålet. Fritextfält undviks.

- I de fall där fritextfält inte kan undvikas, bör användaren i själva gränssnittet ges en påminnelse om att vara integritetsmedveten ifråga om vilka uppgifter eller formuleringar som förs in och begränsa uppgifterna till enbart det som är nödvändigt.
- Särskilt känslig personlig information utelämnas helt i den mån uppgiften inte är helt nödvändig för syftet med behandlingen. (Känslig personlig information kan vara information om ras eller etnisk bakgrund, politisk eller religiös uppfattning, hälsa, sexuell läggning, medlemskap i fack-föreningar eller att en person har blivit misstänkt eller dömd för brott.)
- Personnummer utelämnas om det inte är nödvändigt för ändamålet med behandlingen.
- Känslig information döljs bakom ett ”extra klick” (t.ex. en flik eller länk eller genom att en popup-ruta kräver att användaren bekräftar) för att bli synlig, så att den känsliga informationen inte är det första som en användare ser när man söker på en viss person i systemet. Detta ger dessutom möjligheter att kunna logga vilka användare som varit inne och sett just den känsliga informationen. Beroende på sammanhanget kan den registrerades namn i sig vara en mycket känslig uppgift och behöva döljas på detta sätt (t.ex. i ett HR-system som listar personer som är under rehabilitering för alkohol- och drogproblem).

Följande åtgärder ska övervägas med hänsyn till riskerna med behandlingen. Åtminstone vid behandling av känslig information bör åtgärderna betraktas som obligatoriska:

- Enbart uppgifter som *indirekt* kan identifiera personen registreras. Med att en person är indirekt identifierbar avses om det är möjligt att identifiera personen genom bakgrundsinformation såsom tillhörighet till visst företag, organisation, bostad eller liknande kombinerad med information om ålder, kön, yrke, diagnos etc.
- Namn och/eller personnummer ersätts av pseudonym, som exempelvis kundnummer.
- Lagrad information krypteras för att begränsa tillgången.
- Automatiska gallringsrutiner etableras så att information raderas enligt ett specifikt tidsintervall eller när syftet med behandlingen inte längre är för handen.

4. Se inte personlig integritet som ett nollsummespel

Skyddandet av personuppgifter ska inte vara en börda för utvecklaren; istället för att offra funktionalitet bör man istället tänka på hur privacy kan tillvaratas på ett sådant sätt att en ”win-win-situation” uppstår. Ett exempel är att i system för telefonkundtjänst låta kunden identifiera sig med tonval, så att systemet automatiskt öppnar rätt person i systemet för kundtjänstpersonen.

5. Tänk på informationssäkerhet under hela livscykeln

Exempel på lämpliga åtgärder och funktioner, att applicera beroende på riskbilden med behandlingen:

- Det finns åtkomstautentisering med starka lösenord, rutiner och funktioner för säker hantering, samt möjligheter att ansluta systemet till en extern kontohanterare.
- Ett starkt lösenord består av 8 eller flera tecken, vilket är en stor bokstav, samt siffror och tecken. Inga hela ord bör ensamma kunna accepteras som fullständigt lösenord
- Krypterad kommunikation tillämpas via Internet, i databaser och på mobila enheter
- Det loggas automatiskt vem som tittar på vilken personlig information (s.k. tittlogg).
- Det loggas automatiskt vilka ändringar persondata som gjorts och av vem (ändringslogg).
- Det finns etablerade förfaranden för säkerhet och integritet.
- De etablerade säkerhets- och integritetsrutinerna dokumenteras.
- Systemanvändare har blivit bekanta med säkerhets- och sekretesspraxis.
- Det finns stöd för backupgenerering.
- Säkerhetskopiering och säkerhetskopiering är säkrad på samma nivå som andra system. Det finns en plan för säker avveckling av systemet.
- Den säkra avvecklingsplanen innehåller metod för att ta bort och förstöra lagringsmedia.
- Rutiner har fastställts för årlig riskbedömning av systemet.
- Riskbedömningsprocedurer har fastställts för förändringar i systemet.

6. Eftersträva synlighet och transparens i alla lägen

Det rekommenderas att det finns funktionalitet som ger lättillgänglig information för den registrerade personen om hur informationen behandlas i systemet/processen. Informationen ger den registrerade personen meddelande om vilken information som samlas in, hur uppgifterna används, vem som har tillgång till dem, hur och hur länge de lagras, den registrerade personens förmåga att ändra och radera dem och eventuellt vem informationen kan lämnas till. Denna information är tillgänglig både innan personen är registrerad och efter att informationen väl är lagrad. Det finns ett system för samtycke och återkallande av samtycke för insamling av personlig information. Det finns lösningar som tar emot den registrerades begäran om tillgång till registerutdrag eller ger den registrerade åtkomst i inloggat läge för att se vilken personlig information som är registrerad om henne eller honom.

7. Håll alltid användarens integritet i fokus

Det är alltid den enskilda individens intresse som ska stå i centrum när det handlar om hantering av personuppgifter!