SIGNALISTEN

BAKGRUND

Den nya dataskyddsförordningen (General Data Protection Regulation - GDPR) gäller som lag i alla EU:s medlemsländer från och med den 25 maj 2018. Förordningen innehåller 99 artiklar och 173 beaktandesatser. Dessa riktlinjer beskriver varför vi samlar in personuppgifter och hur informationen hanteras.

GDPR ersätter personuppgiftslagen (PUL). GDPR kompletteras med en ny svensk dataskyddslag. Dataskyddslagen förtydligar under vilka förutsättningar personuppgifter får behandlas med stöd av GDPR. Vidare anges i lagen att även stat och kommun ska kunna åläggas att betala sanktionsavgifter vid överträdelser av GDPR samt att GDPR och den nya dataskyddslagen inte ska tillämpas i den utsträckning det strider mot tryckfrihetsförordningen (TF) eller yttrandefrihetsgrundlagen (YGL).

Många av GDPRs begrepp och principer är samma som i PUL. GDPR innehåller en del förändringar och vissa helt nya bestämmelser. Den personuppgiftsansvariges ansvar och skyldigheter förtydligas och utökas och de registrerades rättigheter förstärks.

En annan viktig nyhet i GDPR är att Datainspektionen, som är tillsynsmyndighet i Sverige, kommer att ges möjlighet att döma ut administrativa sanktionsavgifter vid överträdelser av GDPR. Både personuppgiftsansvariga och personuppgiftsbiträden kan påföras sanktionsavgifter. Hur hög sanktionsavgiften blir beror dels på vilken bestämmelse överträdelsen gäller, dels på omständigheterna i det enskilda fallet. Avgiften kan som mest uppgå till 20 miljoner euro eller fyra procent av en organisations årsomsättning, beroende på vilket belopp som är högst.

Definitioner och begrepp

Personuppgiftsansvarig (PuA)
Personuppgiftsansvarig: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

Personuppgiftsbiträde (PuB)
Personuppgiftsbiträde: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Personuppgifter
Personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk levande person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

Behandling
Behandling: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom

insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring

Särskilda kategorier av personuppgifter
Särskilda kategorier av personuppgifter (känsliga personuppgifter): personuppgifter som avslöjar

- ras eller etniskt ursprung,
- politiska åsikter, religiös eller filosofisk övertygelse
- medlemskap i fackförening
- behandling av genetiska uppgifter,
- biometriska uppgifter för att entydigt identifiera en fysisk person,
- uppgifter om hälsa
- uppgifter om en fysisk persons sexualliv eller sexuella läggning.

Behandling av känsliga uppgifter är som huvudregel förbjudet men det finns det möjlighet att behandla dessa uppgifter om vissa förutsättningar föreligger. (Se vidare nedan).

Hantering av personuppgifter – generella riktlinjer
Det är i GDPRs andra kapitel – Principer – artiklarna 5 till och med 11 som det anges när behandling av personuppgifter är tillåten. Det är främst artiklarna 5, 6, 7, 9 och 10 som är aktuella för vår verksamhet.

Principer för behandling av personuppgifter
Artikel 5 i GDPR innehåller generella principer som gäller för all personuppgiftsbehandling.

Vid behandling av personuppgifter ska den personuppgiftsansvarige tillse att uppgifterna:

- behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade
- samlas in för särskilda, uttryckligt angivna och berättigade ändamål. De ska inte senare behandlas på ett sätt som är oförenligt med dessa ändamål – ändamålsbegränsning.
- ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas – uppgiftsminimering.
- är korrekta och om nödvändigt uppdaterade. Felaktiga uppgifter ska raderas eller rättas utan dröjsmål – korrekthet.
- får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka uppgifterna behandlas – lagringsminimering.
- behandlas på ett sätt som säkerställer lämplig säkerhet för uppgifterna – integritet och konfidentialitet.

Den personuppgiftsansvarige ska också ansvara för och kunna visa att dessa principer efterlevs – ansvarsskyldighet.

Laglig behandling av personuppgifter
Av artikel 6 i GDPR framgår när behandling av personuppgifter är laglig.

Behandling är laglig om åtminstone ett av de uppräknade villkoren är uppfyllda. De villkor som anges är i korthet:

Den registrerade har lämnat sitt samtycke för ett eller flera specifika ändamål
eller behandlingen är nödvändig för att:

- fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås
- fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige
- skydda intressen som är av grundläggande betydelse för den registrerade eller annan fysisk person
- utföra en uppgift av allmänt intresse eller som led i den personuppgiftsansvariges myndighetsutövning
- ändamål som rör den personuppgiftsansvarige, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter – intresseavvägning.

Behandling av s.k. ”särskilda kategorier” av personuppgifter
Utgångspunkten i artikel 9 i GDPR är att behandling av vissa personuppgifter är förbjuden. Med särskilda kategorier av personuppgifter avses bl.a. sådana som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller uppgifter om hälsa.

Det är trots förbudet tillåtet att behandla sådana personuppgifter om bland annat följande förutsättningar föreligger:

- den registrerade har lämnat sitt uttryckliga samtycke till behandlingen av dessa uppgifter för ett eller flera specifika ändamål

- behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd

- behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke

- behandlingen utförs inom ramen för berättigad verksamhet med lämpliga skyddsåtgärder hos en stiftelse, en förening eller annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte

- behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade

- behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolars dömande verksamhet

- behandlingen är nödvändig av hänsyn till ett allmänt viktigt intresse – krav på proportionalitetsbedömning

- behandlingen är nödvändig för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål m.m.

Registrerades rättigheter
Rätt till information
Den registrerade har rätt till information när uppgifterna samlas in. I GDPR anges ett antal krav som måste vara uppfyllda.

Det uppställs lite olika krav på informationen beroende på om personuppgifterna samlats in från den registrerade själv eller från annan än den registrerade.

Information ska lämnas om
a) Personuppgiftsansvarig
b) Dataskyddsombud i förekommande fall
c) Ändamålen med behandlingen
d) De kategorier av personuppgifter som behandlingen gäller (om uppgifterna samlas in från annan än den registrerade)
e) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut
f) Rättslig grund
g) Intresse vid intresseavvägning
h) Överföring av uppgifter till tredjeland
i) Hur länge uppgifterna sparas.
j) De registrerades rättigheter (innefattande bland annat rätten att begära rättelse eller radering av personuppgifterna)
k) Rätten att återkalla samtycke
l) Rätten att inge klagomål till en Datainspektionen
m) Uppgiftsskyldighet enligt avtal eller lag
n) Varifrån uppgifterna kommer (om uppgifterna samlas in från annan än den registrerade)
o) Förekomsten av automatiserat beslutsfattande, inbegripet profilering.

Rätt till tillgång
Den registrerade ska ha rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i sådant fall få tillgång till personuppgifterna och följande information:
a) Ändamålen med behandlingen.
b) De kategorier av personuppgifter som behandlingen gäller.
c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut.
d) Hur länge uppgifterna sparas.
e) Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling.
f) Rätten att inge klagomål till en tillsynsmyndighet.
g) Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån uppgifterna kommer.
h) Förekomsten av automatiserat beslutsfattande, inbegripet profilering.

Om personuppgifterna överförs till ett tredjeland ska den registrerade ha rätt till information om de lämpliga skyddsåtgärder som har vidtagits vid överföringen.

Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling (s.k. registerutdrag). För eventuella ytterligare kopior som den registrerade begär får den personuppgiftsansvarige ta ut en rimlig avgift på grundval av de administrativa kostnaderna. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat. Utlämnande av information får inte inverka menligt på andras rättigheter och friheter.

Rätten till rättelse
Alla personer som hanteras av Signalisten har rätt att få sina personuppgifter rättade/ändrade Den registrerade ska ha rätt att av den personuppgiftsansvarige utan onödigt dröjsmål få felaktiga personuppgifter som rör hen rättade. Med beaktande av ändamålet med behandlingen, ska den registrerade ha rätt att komplettera ofullständiga personuppgifter.

Rätten att bli glömd
Alla personer som hanteras av Signalisten har rätt att bli glömda/raderade från alla system och servrar under förutsättning att.a) personuppgifterna inte längre är nödvändiga för de ändamål för vilka de samlats in eller på annat sätt behandlats, b) den registrerade återkallar sitt samtycke i de fall behandlingen grundar sig på samtycke, c) den registrerade invänder mot behandlingen och det saknas berättigade skäl för behandlingen som väger tyngre, d) personuppgifterna har behandlats på ett olagligt sätt, e) personuppgifterna måste raderas för att uppfylla en rättslig förpliktelse som den personuppgiftsansvarige omfattas av.

Om den personuppgiftsansvarige har offentliggjort personuppgifterna och är skyldig att radera personuppgifterna, ska den personuppgiftsansvarige med beaktande av tillgänglig teknik och kostnaden för genomförandet vidta rimliga åtgärder, inbegripet tekniska åtgärder, för att underrätta personuppgiftsansvariga som behandlar personuppgifterna om att den registrerade har begärt att de ska radera eventuella länkar till, eller kopior eller reproduktioner av dessa personuppgifter.

Radering ska inte ske om behandlingen är nödvändig a) för att utöva rätten till yttrande- och informationsfrihet, b) för att uppfylla en rättslig förpliktelse som den personuppgiftsansvarige omfattas av eller för att utföra en uppgift av allmänt intresse, c) för arkivändamål av allmänt intresse eller statistiska ändamål d) för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

Invändning/begränsning
Den registrerade ska ha rätt att av den personuppgiftsansvarige kräva att behandlingen begränsas om något av följande alternativ är tillämpligt:
a) Den registrerade bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige möjlighet att kontrollera om personuppgifterna är korrekta.
b) Behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.
c) Den personuppgiftsansvarige behöver inte längre personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.
d) Den registrerade har invänt mot behandling i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

Om behandlingen har begränsats får ändå sådana uppgifter behandlas som är nödvändiga för att för att fastställa, göra gällande eller försvara rättsliga anspråk.

Dataportabilitet
Om behandling grundas på avtal eller samtycke äger den registrerade rätt till s.k. dataportabilitet. Detta innebär att den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit den personuppgiftsansvarige i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till annan personuppgiftsansvarig utan att den personuppgiftsansvarig utan att den personuppgiftsansvarige som tillhandahållits uppgifterna hindrar detta. Den registrerade kan också begära att uppgifterna förs över till en annan personuppgiftsansvarig.

Incidentrapportering
Rutinerna för incidentrapportering ska vara väl kända inom organisationen.

Incidenthantering
Enligt artikel 4 i GDPR är personuppgiftsincident 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.

I artikel 5.1 f) GDPR anges att personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet). Med förstöring menas att informationen inte längre finns överhuvudtaget eller inte längre finns i någon form som innebär att den kan användas av den personuppgiftsansvarige. Skada innebär att personuppgifter har ändrats, skadats eller inte längre är kompletta. Förlust av personuppgifter ska tolkas som att informationen finns kvar men att den personuppgiftsansvarige har förlorat kontrollen eller tillgången till informationen eller inte längre har den i sin besittning.

GDPR ställer höga krav på incidenthanteringen. Beslutet att rapportering ska ske till Datainspektionen ligger hos stiftelsens ledning. Sådant beslut måste tas i varje enskilt fall. Vad som ska ingå i informationen som skickas till Datainspektionen listas i GDPR och Datainspektionens dokument. Internt bör personalen veta vad som är en incident och vem man vänder sig till för att rapportera incidenten.

Om det inträffar en säkerhetsincident som rör personuppgifter, t.ex. ett dataintrång eller en oavsiktlig förlust av personuppgifter, måste incidenten dokumenteras och anmälas till Datainspektionen inom 72 timmar från det att vi fick kännedom om incidenten. De registrerade kan också behöva informeras t.ex. om det finns risk för id-stöld eller bedrägeri. För att kunna leva upp till de nya skyldigheterna enligt GDPR är det viktigt att de som behandlar personuppgifter har tillräckliga rutiner på plats för att kunna upptäcka, rapportera och utreda personuppgiftsincidenter.

Det finns olika typer av personuppgiftsincidenter t.ex. konfidentialitetsincident – vid obehörigt eller oavsiktligt utlämnande av personuppgifter eller då någon som ej har rätt till det har beretts tillgång till uppgifterna, tillgänglighetsincident – oavsiktlig eller obehörig förlust av tillgång till eller förstörelse av personuppgifter, integritetsincident – obehörig eller oavsiktlig ändring av personuppgifter. Beroende på omständigheterna i det enskilda fallet kan en och samma incident

innefatta flera av de ovan nämnda kategorierna. Det torde vara relativt enkelt att bedöma om det har skett en konfidentialitets- eller integritetsincident. Det kan vara svårare att bedöma om en tillgänglighetsincident har inträffat. Nedan ges några exempel.

1. Förlust av tillgång till personuppgifter kan föreligga när information har raderats antingen oavsiktligt eller av en obehörig person, eller vad gäller krypterade uppgifter, om krypteringsnyckeln har förkommit. Om den personuppgiftsansvarige inte kan återskapa tillgång till uppgifterna, t.ex. via en back up, är detta att anse som en permanent förlust av tillgänglighet.
2. En tillgänglighetsincident kan också uppkomma om det har förevarit ett betydande avbrott i organisationens normala verksamhet, t.ex. i fall av strömavbrott eller en attack mot datasystemet i syfte att hindra normal användning av detsamma (såsom en överbelastningsattack, där systemet kommer att använda någon knapp resurs (nästan) enbart till att hantera data genererat genom attacken) som leder till att personuppgifter inte finns tillgängliga antingen permanent eller tillfälligt.

Ransomware-attacker kan innebära tillfällig förlust av tillgänglighet till data om informationen kan återställas från back up. Rapportering av incidenten kan krävas om utpressaren har fått tillgång till personuppgifter och detta innebär en risk för de registrerades rättigheter.

Personuppgiftsbiträdesavtal

I de fall en extern part har tillgång till eller hanterar personuppgifter åt Signalisten ska ett personuppgiftsbiträdesavtal vara upprättat. Ansvarig för att ett biträdesavtal är upprättat är respektive chef inom respektive avdelning. Se mall för biträdesavtal. Avtalet ska innehålla information om:

- Vem som är personuppgiftsansvarig och organisationsnummer
- Vem som är personuppgiftsbiträde och organisationsnummer
- Föremål för behandlingen
- Hur länge behandlingen ska pågå, vilken/vilka sorts behandlingar och behandlingarnas ändamål
- Typen av personuppgifter
- Kategorier av registrerade (t.ex. anställda, hyresgäster)
- Personuppgiftsansvariges skyldigheter och rättigheter
- Att personuppgiftsbiträdet ser till att den personuppgiftsansvariges skyldigheter fullgörs, t.ex. att kunna visa att biträdet verkligen vidtar lämpliga skyddsåtgärder
- Att behandling bara får göras i enlighet med instruktioner från den personuppgiftsansvarige, inklusive överföring till tredje land
- Att personerna som behandlar uppgifterna har ingått avtal om konfidentialitet eller lyder under lagstadgad tystnadsplikt
- Att personuppgiftsbiträdet har lämplig säkerhetsnivå för att skydda uppgifterna
- Att biträdet ska underrätta den personuppgiftsansvarige om en personuppgiftsincident inträffar
- Att förhandstillstånd krävs om ett underbiträde ska anlitas (ett s.k. underbiträde)
- Assistans med att svara upp mot att de registrerades rättigheter säkerställs
- Åtgärder när samarbetet mellan personuppgiftsansvarige och personuppgiftsbiträdet upphör, som att personuppgifter ska raderas eller lämnas tillbaka
- Ge tillgång till nödvändig information åt den personuppgiftsansvarige
- Möjliggöra och bidra till granskningar och inspektioner.

E-post

Följande gäller vid intern hantering av personuppgifter med e-post:

- I den absoluta mån det går ska personuppgifter inte skickas via e-post.
- Går det att avidentifiera/maska personuppgifterna ska det göras
- E-post som inkommer (och som inte är allmänna handlingar) som innehåller personuppgifter får ej sparas utan anledning
- I e-postbrevlådan får ingen lagring av personuppgifter ske

En viktig förändring när GDPR börjar tillämpas är att den s.k. missbruksregeln i PUL försvinner.

Vad innebär missbruksregeln?

Enligt 5 a § i PUL görs undantag från de viktigaste bestämmelserna i PUL för behandling av personuppgifter i ostrukturerat material förutsatt att behandlingen inte kränker den registrerades integritet, den s k missbruksregeln. Den har utgjort ett stöd för att personuppgifter har kunnat behandlas i löpande text eller i bilder i mejl, på hemsidor, i sociala medier m.m. När GDPR börjar tillämpas kommer inte längre denna regel att finnas kvar. Det görs alltså inte längre något undantag för personuppgiftsbehandling i ostrukturerat material.

Teknisk säkerhet

Signalisten ska i alla lägen upprätta och bevara de tekniska och organisatoriska åtgärder som krävs för att skydda samtliga personuppgifter.

Fysiska skyddet

IT-utrustning som används för behandling av personuppgifter ska ha ett tillfredsställande skydd mot stöld och händelser som kan förstöra utrustningen.

Vilka Signalisten delar personuppgifter med

Signalisten överför eller delar inga personuppgifter med tredje part om inte ett personuppgiftsbiträdesavtal upprättats.

Personuppgifter kan dock få lämnas ut när stiftelsen fullgör sina skyldigheter eller utövar sina rättigheter inom arbetsrätten.

För att uppgifterna i andra sammanhang ska få lämnas ut till tredje man utan uttryckligt samtycke krävs att utlämnandet är nödvändigt för att rättsliga anspråk ska kunna fastställas eller göras gällande.

Vilket ansvar och vilka rättigheter har Signalisten?

Signalisten ska i alla lägen upprätta och bevara de tekniska och organisatoriska åtgärder som krävs för att skydda samtliga personuppgifter. Vidare ska Signalisten behandla personuppgifter för vilka Signalisten är personuppgiftsbiträde i enlighet med personuppgiftsansvariges instruktioner och GDPR samt den kompletterande svenska dataskyddslagen.

Tredje land

Signalisten överför eller behandlar inga personuppgifter i tredje land, dvs. land utanför EU/EES.