Informationssäkerhet och Dataskyddsarbete

Johnny Lundström
IT-Koordinator/Dataskyddsombud
Region Västerbotten

Varför nya regler

- Modernisering – Nu gällande regler bygger på ett direktiv från 1995
- Datamängderna växer (mobilt internet. Internet of things)
- Skapa enhetliga dataskyddsregler inom hela EU (Single Digital Market)
  Harmonisering – Samma rättigheter och skyldigheter i hel EU/EES
- Starkare skydd för den personliga integriteten för EU:s medborgare
  Förstärkning av **enskildas rättigheter** och **tydliggörande av ansvar och skyldigheter** för **den** som behandlar personuppgifter

Grundläggande principer för behandling

- Laglighet och **öppenhet**
- Ändamålsbegränsning
- Uppgiftsminimering
- Korrekthet
- Lagringsminiering
- **Integritet och konfidentialitet**

Den personuppgiftsansvarige ska ansvara för och kunna visa att punkterna efterlevs - **Ansvarsskyldighet**

Nyheter i korthet

- Tillsyn och föreläggande om GDPR ej efterlevs
- Registrerades rättigheter förstärks
- Nya regler för barn över 13 år (Med stöd av barnets samtycke)
- Information om datalagring ska kunna ges i digitalt format
- Dataportabilitet
- Utökat ansvar för personuppgiftsbiträden
- Krav på en tydlig organisation, strategier och styrande dokument
- Rapporteringskrav vid IT-incidenter
- Utökat informationskrav till de registrerade (kunder, anställda, offentlighet)
- Hårdare regler för marknadsföring och profilering
- Krav på konsekvensbedömning (dataskyddsanalys) vid förändringar i personuppgiftsbehandlingen
- Krav på inbyggt dataskydd i IT-systemen (Privacy by design)

Planering för övergripande åtgärdsplan

- Ta **beslut** i verksamhetsledning om att dataskyddsfrågorna ska prioriteras
- Ta fram en **övergripande strategi** för dataskyddsarbetet
- Säkerställ **verktyg** eller säker lagring för organisationen
- Skicka ut informationsbrev och kalla all personal som tror sig arbeta med register för en första introduktion och genomför **utbildningsinsatser** för de anställda om dataskyddsregler
- Analys och dokumentation av **säkerhetsåtgärder** för IT-system
- Tänk igenom hur organisationen ser ut och fundera igenom vilka tänkbara register som kan finnas och varför dessa register finns.

- **Fundera på och granska de avtal som finns och till dem kopplade biträdesavtal**

Dataskyddsombudet leder projektet och samlar in information från de olika avdelningarna men berörd personal måste vara med i hela processen.

Påbörja inventeringen

Inventeringens syfte är att få en överblick som innebär:

- Registrering av behandling av personuppgifter där vår verksamhet är personuppgiftsansvarig.
- Varje enskild behandling ska registreras separat och ges ett eget namn, för att underlätta sorteringen.
- Inventeringen hjälper oss följa principen om ansvarsskyldighet i GDPR

- Information efterfrågas enligt nuvarande lagstiftning och kommande dataskyddslagstiftning (GDPR).
  (Region Västerbotten utgår från att följa kommande lagstiftning för GDPR redan idag.)

- Vissa frågor är obligatoriska medan andra är frivilliga.

- Hjälptexter och hänvisningar till relevanta lagar ger dig vägledning

Utvärdering

- Behandlingen är laglig eller ej
- Att alla informationsinsatser har genomförts
- Tydliga gallringsrutiner(ska informeras om vid första träff)
- Rutiner för hur behandlingen utförs

Utvärdering så snart som möjligt efter inventeringen. Noga med att återkoppla till respektive avdelning/enhet/person om vad som framkommit genom inventeringen.

Målet: Säkerställa om personuppgiftsbehandlingarna är lagliga, att de följer god sed, att gallringsrutiner finns m.m.

En utvärdering ska göras på allt material som samlats in och resultatet återkopplas till berörda och till organisationens ledning **direkt efter genomförd inventering för förslag till åtgärder.**

Rapport till ledningen

Det är alltid organisationsnumret (den juridiska personen som företräder organisationen) som har det yttersta ansvaret för genomförande av åtgärder. Det är inte de enskilda medarbetarna.

Behövs det måste resurser, tid mm tilldelas för att åtgärda fel.

Lämna en skriftlig rapport

Beskrivning av rapportinnehållet och förklaring för berörda chefer under ett möte där man avsätter särskild tid för detta.

Åtgärdsplan

När inventeringen och utvärderingen är gjord är det dags att sammanfatta slutsatserna av inventeringen och ta fram en åtgärdsplan.

Åtgärdsplan och sammanfattning ska:

- Vara tydlig och fokusera på frågorna, vad, varför, hur och vem?
- I första hand att se till att behandlingen är tillåten enligt PuL/GDPR
- I andra hand kan det även gälla att ta fram policydokument, FAQ för användarna, information på intranätet
- Informera ledningen angående legala frågor
- Tekniska åtgärder

Åtgärdsplan vid problem

Organisationen är alltid ägare av ev. problem som presenteras i problemområdena för till exempel systemägaren eller informationsägaren.

Dataskyddsombudet är att betrakta som en ”internrevisor” som pekar på problemet.

Av åtgärdsplanen bör det framgå:

- vilken behandling som avses,
- vilket eller vilka problem som behöver lösas och varför,
- hur problemet är tänkt att lösas,
- vilka resurser som ska vidta åtgärderna (anställda, konsulter, biträdet),
- när problemet ska vara löst,
- hur åtgärderna ska rapporteras,
- till vem de ska rapporteras,
- vem som ansvarar för att det blir gjort.

Registerförteckning

Registerförteckningen ska innehålla en registerbeskrivning över varje behandling av personuppgifter i organisationen vad gäller

- Syfte/ändamål - varför man registrerar **personnummer** och/eller **känsliga personuppgifter**
- Innehåll
- Personuppgiftsansvariges **namn, adress, telefonnummer och org.nummer**
- Beskrivning av den/de uppgifter/kategorier av registrerade som berörs/behandlas
- Uppgift om mottagarna eller de kategorier av **mottagare till vilka uppgifterna kan komma att lämnas ut**
- Upplysning om överföringar av uppgifter till **tredjeland**
- Allmän beskrivning av de åtgärder som har vidtagits för att trygga **säkerheten** i behandlingen.
- Rutiner för gallring och behörighetstilldelning

Tänk dock på att registerförteckningen förmodligen är en allmän handling. Man bör inte beskriva säkerhetsåtgärderna mer än på ett generellt sätt och det kanske är mindre lämpligt att i registerförteckningen notera saker som inte fungerar tillfredsställande.

Registerförteckning

Kan upprättas på papper i en pärm (om registerbeskrivningarna är få), eller som ett IT-baserat system. Det senare väljer man om det är troligt att det kommer att upprättas så många olika registerbeskrivningar att det kommer att bli nödvändigt att göra sökningar på ändamål, kategori av registrerade, systemägare eller liknande.

Stort problem kan kräva en förstudie

Gäller det ett större problem kan en förstudie behöva göras, framförallt vad gäller kostnader.

Det kan också bli nödvändigt att kontrollera med Datainspektionen för att **få prövat** om den föreslagna lösningen är tillräckligt bra.

Viktiga länkar

Myndigheten för samhällsskydd och beredskap:
https://www.msb.se/sv/Forebyggande/Informationssakerhet/

Datainspektionen:
http://www.datainspektionen.se/dataskyddsreformen/

Förvaltning ska säkerställas i form av

- Rutiner och kontaktnät
- Rutinbeskrivningar. Bra rutinbeskrivningar betyder mindre arbete och mindre risk för fel i framtiden.

- **Rutiner bör därför finnas för:**
- Uppdatering av registerförteckningen
- Ta fram registerutdrag
- Gallring
- Behörighetstilldelningen
- Andra i organisationen har rutiner som säkerställer att integritetsskyddsfrågorna beaktas.

Tänk på:
Viktigt för dataskyddsombud att vara med från början i de olika projekt som rör IT-frågor och register för att få möjlighet att lämna synpunkter utifrån en integritetsskyddsaspekt.
Det är viktigt att bli engagerad på ett tidigt stadium – särskilt om det startas upp en projektgrupp.

Många och känsliga personuppgifter registreras på personalavdelningen. Dataskyddsarbetet måste omfatta HR-avdelningens arbete och det är därför synnerligen viktigt att personuppgiftsombudet har insyn i personalarbetet och kan komma med synpunkter på hur registreringen av de känsliga personuppgifterna ska behandlas.

Tack för din medverkan!

Länk till samlande dokument och genomgångar

https://drive.google.com/drive/folders/0B-nrl8AMwH0RYnNzcEllVXNBS0U

Johnny Lundström IT-Koordinator/Dataskyddsombud

Region Västerbotten

REGION VÄSTERBOTTEN

Dataskydd – Listor & Evenemang

Anmälningslistor och evenemang

Vad som ska finnas med i förteckningen framgår uttryckligen i artikel 30 nya GDPR, tex:

- Ändamålen med behandlingen
- Beskrivning av kategorierna av registrerade
- Kategorierna av personuppgifter
- Eventuella mottagare av personuppgifterna.
- Samtycke

Kom ihåg
Rätt till information
Rätt till rättelse
Rätt till radering ("rätten att bli bortglömd")
Rätt till begränsning av behandling
Dataportabilitet
Rätt att göra invändningar
Automatiserat beslutsfattande, inbegripet profilering
Samtycke(Ett samtycke ska vara en otvetydig viljeyttring)

Det är behandlingen som sådan som ska framgå i förteckningen, utan vilka uppgifter man behandlar, hur och varför.
INTE nödvändigt att dokumentera varje nytt evenemang för sig, förutsatt att inte ändamålen/syftet ändras.

MEN:
Bestämmelserna i EU:s dataskyddsförordning innebär att missbruksregeln kommer att upphöra, vilket innebär att förordningens alla regler om personuppgiftsbehandling ska tillämpas även vid s.k. ostrukturerad behandling, se mer i följande länk:
http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-upphor/

Vidare har ”intresseavvägning” ett begränsat användningsområde som rättslig grund för myndigheter
http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/rattslig-grund-for-personuppgiftsbehandling/intresseavvagning/

REGION VÄSTERBOTTEN

Dataskydd – Mobiltelefoner

Om jag som anställd använder en privat telefon i tjänsten och lägger in epost och andra uppgifter i min privata mobil, vad gäller då enligt GDPR?
Är detta lagligt?

Man måste ställa sig frågan:

- Vem är personuppgiftsansvarig
- Hur skiljer man på dessa saker.
- Vilken laglig grund, eftersom missbruksregeln försvinner
- Behandling av tjänsterelaterad information, faller ej under privatundantaget.
- Hur ska man då se till att reglerna följs när det inte är utrustning som arbetsgivaren kontrollerar eller kan påverka. som arbetsgivaren har ett ansvar över.

Finns ingen lätt lösning
Kan man ha en lösning där man kan separera delarna?
Tjänstemail är en separat app i telefonen och avskild från övrig data

Tydliga instruktioner (Policy) och riskbedömning måste upprättas - OM den ska användas för tjänsteärenden.

REGION VÄSTERBOTTEN

Dataskydd - Bibliotek

Bibliotek ute i landet ska kunna erbjuda och erbjuder läsmöjligheter i flera former och det finns offentliga datorer och plattor på våra bibliotek

Hur ställer sig lagen/Nya GDPR till denna fråga om man vill vara anonym?

Om ett bibliotek (ansvarig nämnd är personuppgiftsansvarig) behandlar personuppgifter genom att till exempel logga vem som använder en dator på ett bibliotek måste det finnas **ett rättsligt stöd** för detta och följa **de grundläggande principerna** i dataskyddsförordningen:

Laglighet, korrekthet och öppenhet
Ändamålsbegränsning
Uppgiftsminimering
Korrekthet
Lagringsminimering
Integritet och konfidentialitet
Ansvarsskyldighet

Självfallet måste övriga bestämmelser i dataskyddsförordningen också följas.

Först och främst måste ansvarig nämnd/organisation/kommun bestämma för vilket eller vilka ändamål som personuppgifterna ska behandlas och sedan kontrollera att det finns ett rättsligt stöd för en sådan behandling.

Biblioteket måste även beakta de starka bestämmelser om sekretess som råder inom biblioteksverksamheten

REGION VÄSTERBOTTEN

Dataskydd – Ägande av data

Förhållandet mellan en kommuns organisationsnummer och de nämnder som finns i ex en kommun eller organisation..

Vem blir den juridiska personen och därtill personuppgiftsansvarig när förhållandet i en kommunen som har ett eget organisationsnummer, men ex. socialnämnden som också lyder under kommunstyrelsen säger sig ha eget ansvar, gäller det även andra nämnder eller verksamheter i en kommunal verksamhet. Vari ligger personuppgiftsansvaret på behandling av data? Regleras detta av subsidära lagar eller är det i slutändan kommunfullmäktige/org.numret som är ansvarig?

Svar:
Personuppgiftsansvaret i en kommun ligger normalt hos de kommunala nämnder som är så självständiga att de **är förvaltningsmyndigheter.** En kommunal nämnd som är förvaltningsmyndighet är således personuppgiftsansvarig för de behandlingar av personuppgifter som nämnden har att utföra.

När man i en organisation som tex. Region Västerbotten, har bolag som ägs av RV men bolagen har egna org. nummer, eller exempel på bolag som till hälften har extern verksamhet och till hälften intern verksamhet (till ägaren).
Styr organisationsnumret eller ägandet personuppgiftsansvaret ansvaret för behandling av data?

Svar: **Personuppgiftsansvarig är normalt den juridiska person (till exempel aktiebolag, stiftelse eller förening) eller den myndighet som behandlar personuppgifter i sin verksamhet och som bestämmer vilka uppgifter som ska behandlas och vad uppgifterna ska användas till.**

Det är alltså **inte säkert att varken organisationsnummer eller ägande styr, utan vem som kontrollerar behandlingen av personuppgifter.** En annan sak är att det är just den juridiska personen som är ansvarig, inte exempelvis enskilda avdelningar eller medarbetare.

När missbruksregeln försvinner innebär det att **samma regler som gäller för övriga personuppgifter även gäller det som tidigare undantogs i s.k. ostrukturerat material, dvs. såväl minnesanteckningar som e-post.**

Känsliga personuppgifter **bör aldrig** föras över via vanlig e-post. För definition av känsliga personuppgifter enligt förordningen.

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i en fackförening
- Hälsa
- En persons sexualliv eller sexuella läggning
- Genetiska och biometriska uppgifter som entydigt identifierar en person.

För övriga uppgifter, även de som tidigare var undantagna enligt missbruksregeln, gäller att förordningen ska tillämpas i sin helhet på all automatiserad behandling av personuppgifter.
Man kan till exempel behöva undersöka om vi uppfyller de allmänna principerna för behandling av personuppgifter som finns i den kommande dataskyddsförordningens **artikel 5**:
http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/principer-for-behandling-av-personuppgifter/

Till exempel ska inte fler personuppgifter än nödvändigt behandlas samt tiden uppgifterna lagras ska minimeras.

Vidare behöver man ha en **rättslig grund för behandlingen,** som återfinns i artikel 6**. För myndigheter gäller ofta art. 6 c eller e:**
DVS: Nödvändigt för att fullgöra en rättslig förpliktelse resp. nödvändigt för att utföra en uppgift av allmänt intresse eller som ett led i den personuppgiftsansvariges myndighetsutövning. Möjligheten för myndigheter att använda den rättsliga grunden intresseavvägning begränsas kraftigt i och med förordningen.
Här finns mer information om att missbruksregeln försvinner:
http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/missbruksregeln-upphor/

Dataskydd - Webbplats

En webbplats tillhörande en kommun eller myndighet är ju **i normala fall bunden till kommunen/myndigheten vad gäller juridiskt ansvar.**

Offentlighetsprincipen eller Personuppgiftslagen? Vilken lag går före?

En webbplats tillhörande en kommun eller myndighet är ju **i normala fall bunden till kommunen/myndigheten vad gäller juridiskt ansvar.**

Offentlighetsprincipen eller Personuppgiftslagen? Vilken lag går före?

SVAR:

Det är möjligt att myndigheter kan stödja sig på att publiceringen görs för att utföra en uppgift av allmänt intresse, men hur det förhåller sig går inte att slå fast utan att se till omständigheterna.

Dataskyddsförordningen hindrar inte den personuppgiftsbehandling **som är nödvändig för att myndigheter ska kunna uppfylla skyldigheten att lämna ut allmänna handlingar enligt offentlighetsprincipen.**

Detta innebär att om någon vänder sig till myndigheten och begär ut uppgifter med stöd av offentlighetsprincipen och det **inte finns någon sekretessbestämmelse** som hindrar ett utlämnande så måste myndigheten lämna ut uppgifterna till den som begär det.

REGION VÄSTERBOTTEN

Dataskydd - Utgivningsbevis

Utgivningsbevis är en typ av intyg som behövs i vissa fall för att erhålla grundlagsskydd enligt tryckfrihetsförordningen (TF) eller yttrandefrihetsgrundlagen (YGL). Ett sådant kan också vara nödvändigt för att få ge ut exempelvis en tidning. Ett utgivningsbevis gäller i tio år och kan därefter förlängas.

Kan också utfärdas till webbplatser.

Några av kraven som ställs är då att webbplatsen ska ha en ansvarig utgivare, ha anknytning till Sverige, och vara öppen för allmänheten. Med ett utgivningsbevis och grundlagsskydd kan även reglerna i personuppgiftslagen kringgås av en webbsida

Det finns inga hinder för en myndighet att ansöka om utgivningsbevis, men om en myndighet går längre än vad som krävs enligt tryckfrihetsförordningen och yttrandefrihetsgrundlagen, (och det finns ingen skyldighet att webbpublicera, utan endast att lämna ut handlingar efter en begäran från enskild) så måste personuppgiftsbehandlingen uppfylla kraven i personuppgiftslagen och sedermera **dataskyddsförordningen.**