Dataskyddsombudsrollen och Dataskyddsförordningen i korthet

Madeleine Arvidsson Wäli, Dataskyddsombud

Dataskyddsombudsrollen i kommun

GÖTEBORGS REGIONEN

Lag och avtalet som grund

Mitt uppdrag framgår dels av förordningen och dels av samverkansavtalet som tecknats.

Resterande innehåll styrs av efterfrågan.

Överenskommelse finns

- Att vid behov jobba mer i en kommun
- Att dela med sig av det som görs för en kommun till de andra kommunerna

Uppgifter enligt förordningen

- Informera och ge råd till organisationen
- Övervaka efterlevnaden av förordningen, annan dataskydds-lagstiftning och interna styrdokument
- Ge råd om konsekvensbedömning
- Samarbeta med Datainspektionen
- Vara kontaktperson för Datainspektionen

Kunskapsstöd

DSO ska vara ett kunskapsstöd gällande innehåll och tillämplighet av gällande dataskyddsförordning och angränsande regler

DSO ska även omvärldsbevaka frågor rörande dataskyddslagstiftningen

- Informera
- Ge råd till personal
- Identifiera kompetensutvecklingsbehov
- Planera och genomföra utbildning

Stöd i verksamheten

- Arbeta för organisatoriska säkerhetsskyddsåtgärder
- Ge råd vid genomförande av konsekvensbedömning av dataskydd och övervaka genomförande av denna
- Bistå i utredningen av misstänkta dataintrång, personuppgiftsincidenter
- Omvärldsbevaka frågor rörande dataskyddslagstiftningen

Kontaktpunkt

- Kontaktpunkt för tillsynsmyndigheten
- Kontaktperson för de personalen
- (Kontaktperson för de registrerade)
- Vid behov genomföra förhandssamråd

Kontroll

Övervaka den interna efterlevnaden av

- dataskyddslagstiftningen
- organisationens strategi för dataskydd

- Ge råd vid genomförande av konsekvensbedömning av dataskydd och övervaka genomförande av denna
- Arbeta för organisatoriska säkerhetsskyddsåtgärder

Ledningsfrågor

DSO ska arbeta för organisatoriska säkerhetsskyddsåtgärder.

Bistå i utredningen av misstänkta dataintrång.

Rapportera, när så är påkallat, till ledningen

- angående dataskyddsfrågor
- organisatoriska brister
- utvecklingsbehov
- liknande frågor

Ledningsansvar

- Personuppgiftsansvaret ligger på respektive nämnd och styrelse
- Personuppgiftsansvarig fastställer strategier och tillser att lämplig organisation finns
- Ledningsgruppen har förvaltningsansvar
- Skapa gärna en grupp som fortsätter arbetet
- Det kräver resurser i form av tid och budgeterade medel

DSO i praktiken

- Råd och stöd till personalen
- Göra internkontroller av efterlevnaden
- Skapa nätverk för olika personalgrupper

- Finnas på plats regelbundet enligt överenskommelse
  6 och 20 februari
  6 och 20 mars
  3 och 17 april
  15 och 29 maj
  12 och 26 juni

Dataskyddsförordningen i korthet

GÖTEBORGS REGIONEN

Grundläggande begrepp

Personuppgiftsansvarig
Personuppgiftsbiträde
Dataskyddsombud

Personuppgift
Särskild och känslig personuppgift

Allmän handling

Personuppgiftsbehandling
Personuppgiftsincident
Registerförteckning

Rättslig grund för behandling

Sanktionsavgifter

Vem är vem?

Personuppgiftsansvarig

- Kommunstyrelsen
- Nämnder
- Revisionen

Den som bestämmer ändamål och medel för en behandling.

Ansvaret kan inte delegeras.
Aldrig en enskild person.

Personuppgiftsbiträde

- Konsulter
- Systemleverantörer

Den som på uppdrag av en ansvarig utför personuppgiftsbehandling.

Finns alltid utanför den egna organisationen.

Kan vara en enskild person eller en organisation.

Personuppgift

Varje uppgift som avser en identifierad eller identifierbar fysisk nu levande person.

Direkt eller indirekt identifiering.

- Namn
- Kontaktuppgifter
- Personnummer
- Fotografier och ljudupptagning
- E-postadresser
- Cookies och IP-adresser

- Protokoll och anteckningar
- Nyhetsbrevslista

- Taggen

Särskilda kategorier av personuppgifter

- Religiös och filosofisk övertygelse
- Politisk åsikt och fackföreningsmedlemskap
- Ras eller etniskt ursprung
- Sexuell läggning eller sexualliv
- Hälsotillstånd
- Biometri, film och foto
- Genetik

Känsliga personuppgifter

Tidigare kallades uppgifter på förra bilden för känsliga uppgifter.

Numera menar man ofta uppgifter som kräver lite extra skydd.

Exempelvis

- Personnummer
- Kontonummer
- Skuldsättning

Personuppgiftsbehandling

Alla former av hantering och lagring av personuppgifter.

Strukturerat och ostrukturerat.

Både papper och digitalt.

Allt man gör med en uppgift som är kopplad till en fysisk person.

Den enskilde (registrerade) äger sina uppgifter.

Grundläggande principer

Laglighet, korrekthet och öppenhet

Ändamålsbegränsning

Uppgiftsminimering

Riktighet

Lagringsminimering

Integritet och konfidentialitet

Ansvarsskyldighet

- Stöd i dataskyddsförordningen
- Specifika, särskilt angivna och berättigade ändamål
- Inte fler personuppgifter än vad som behövs för ändamålen
- Personuppgifterna ska vara riktiga
- Radera personuppgifterna när de inte längre behövs
- Skydda personuppgifterna
- Visa att och hur ni lever upp till dataskyddsförordningen

Rättslig grund för behandling

Behandlingen är nödvändig

- **Allmänt intresse**
- **Myndighetsutövning**
- **Rättslig förpliktelse**
- **Avtal**

- Grundläggande intressen
- Intresseavvägning

Samtycke

- Aktivt
- Frivilligt
- Specifikt
- Informerat
- Otvetydig viljeyttring

Ett samtycke går att återkalla.

Kräver stora administrativa insatser.

GDPR och OSL

Dokument som har inkommit till eller upprättats vid en myndighet blir allmänna handlingar.

Allmänna handlingar kan vara
- Offentliga
- Sekretessbelagda

Utlämnande av allmän handling ska ske i enlighet med nationell lagstiftning.

Utlämnande av allmän handling ryms inom den rättsliga grunden
- Allmänt intresse

Registerförteckning

Dataskyddsförordningen ställer krav på att alla behandlingar ska finnas nertecknade.

Draftit förteckning

I förteckningen redovisas bland annat

- Rättslig grund
- Ändamål med behandlingen
- Kategorier av personer
- Kategorier av uppgifter
- Lagringsplats
- Gallringsrutiner

GÖTEBORGS REGIONEN

Personuppgiftsincident

En incident är generellt allt som sker med en personuppgift som inte var syftet från början.

I vissa fall ska en incident anmälas till Datainspektionen inom 72 timmar.

- Stöld av dator och telefon
- Förlust av tagg
- Felskickad post, e-post
- Publicering
- Brist på gallring

- Oavsiktlig eller olaglig
  - Förstöring
  - Förlust
  - Ändring
- Obehörigt röjande eller åtkomst
- Gäller personuppgift som
  - Överförs
  - Lagras
  - Behandlas

Incidentrapport

Det finns en rutin för incidentrapport på intranätet.
Läs igenom den i förväg.

Ta reda på vem som är ansvarig för rapporteringen.

Alla händelser ska dokumenteras, diarieföras och anmälas till DSA och DSO.

Stäm av med DSA och DSO om händelsen också ska anmälas till Datainspektionen.

DSA är respektive avdelningschef.

Faran med att göra fel

Anseendet
- Skriverier i media

Skadestånd
- Ingen nyhet egentligen

Sanktionsavgifter
- Kan kompletteras med varning, reprimand och föreläggande

Sanktionsavgifter för myndigheter
- Max 10 milj kronor

Sanktionsavgifter för andra organisationer upp till den högsta summan av

- 20 milj Euro alt 4 % av årsoms
- 10 milj Euro alt 2 % av årsoms

Säkerhet

Var och hur förvaras utrusningen?
- Tillträde till lokaler.

Vem har tillgång till vad?
- Behörighetstilldelning.

Var används mobila enheter?
- Tas mobiler med till tredje land?
- Arbetar man på caféer, tåg eller hotell?

Var sparas information?
- Moln eller källaren?

Hur skickas information?
- E-post kanske bör krypteras.

Tredje land

Att läsa är att behandla!

SKL:s information om Dataskyddsförordningen

https://skl.se/ekonomijuridikstatistik/juridik/offentlighetsekretessarkiv/dataskyddsforordningengdpr.13023.html

https://www.youtube.com/watch?v=0ba-E3B2ebo&feature=youtu.be

Film: GDPR på en minut!

Denna korta film beskriver övergripande vad den nya dataskyddsförordningen, GDPR, innebär.

Datainspektionens information

www.datainspektionen.se

https://www.datainspektionen.se/globalassets/dokument/enkla-grunder-i-dataskydd.pdf

Enkla grunder i dataskydd

2018 fick Sverige och övriga EU en ny gemensam lagstiftning som reglerar hur bland annat företag får behandla personuppgifter. En nyhet i denna dataskyddsförordning är kännbara sanktionsavgifter om man bryter mot reglerna, något som har fått många företag att fundera över hur de hanterar och skyddar personuppgifter. Här följer en grundkurs i dataskydd med fokus på mindre företag.

Dataskydd på 5 röda

Samla inte in fler personuppgifter än nödvändigt och enbart för att visst, i förväg bestämt ändamål. Spara inte uppgifterna längre än nödvändigt. Se till att ni har stöd i lagen för att samla in uppgifterna.

ÄVEN KÄND SOM GDPR

Dataskyddsförordningen kallas ibland kort för GDPR vilket står för General Data Protection Regulation. Förordningen började tillämpas i maj 2018 och ersatte då den svenska personuppgiftslagen.

Vad är egentligen en personuppgift?

Personuppgifter är all slags information som kan knytas till en fysisk person som är i livet. Typiska personuppgifter är personnummer, namn och adress. Även foton på personer klassas som personuppgifter. Ja, till och med ljudinspelningar som lagras elektroniskt kan vara personuppgifter även om det inte nämns några namn i inspelningen. Ett bolagsnummer är ofta inte en personuppgift men är det om det handlar om en enskild näringsverksamhet. Registreringsnumret på en bil kan vara en personuppgift om det går att knyta till en fysisk person medan registreringsnumret på en firmabil som används av flera, kanske inte är en personuppgift.

Detta är en infografik från Datainspektionen. Läs mer om dataskyddsförordningen på www.datainspektionen.se/gdpr

GÖTEBORGS REGIONEN

- Kommer du för att hämta mig?
- Nej, bara ditt samtycke…

GÖTEBORGS REGIONEN

Madeleine Arvidsson Wäli, Dataskyddsombud

madeleine.arvidsson.wali@goteborgsregionen.se

dso@goteborgsregionen.se

031-335 52 53

Anders Perssonsgatan 8, plan 5

Tveka inte att kontakta mig!

GÖTEBORGS REGIONEN