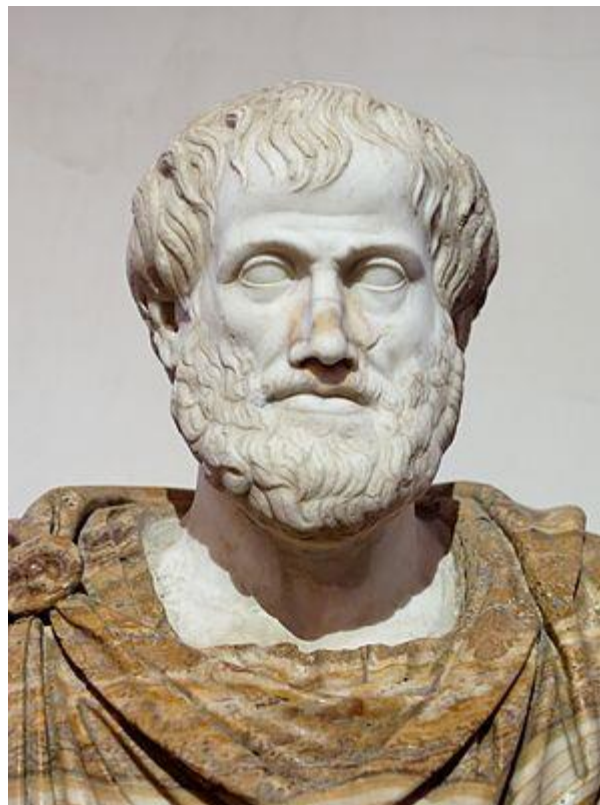


Dataskyddsförordningen (DSF/GDPR)

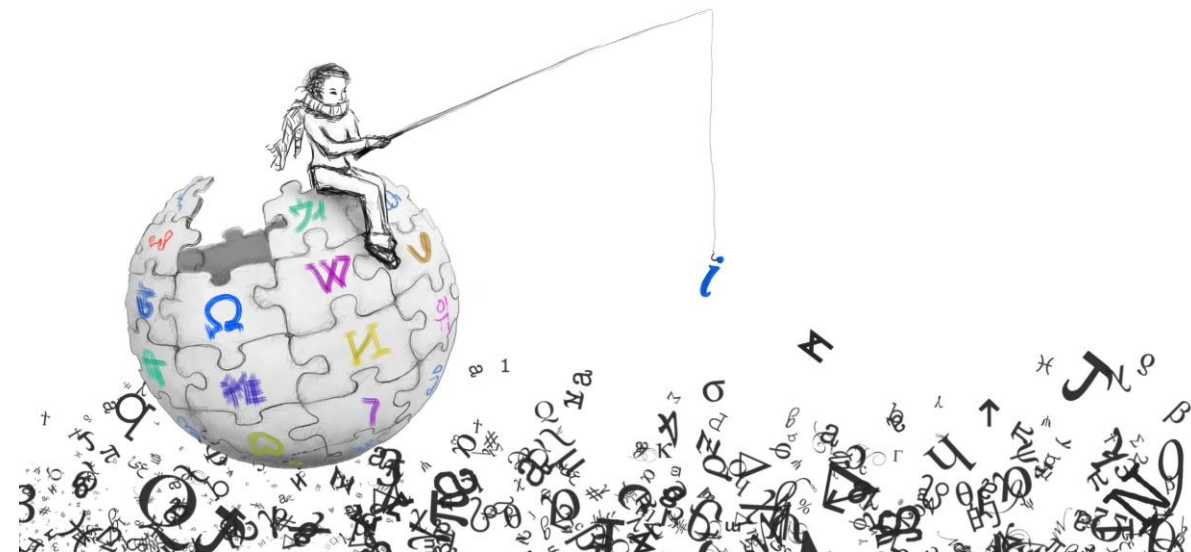
**Styrelseinformation – Bostads AB Poseidon
2018-09-27**

Nina Havner
Dataskyddsombud



Bakgrund Dataskyddsförordningen

- EU beslut i april 2016 om en Dataskyddsförordning (DSF).
- DSF tillämpas från 25 maj 2018 i samtliga medlemsstater.
- Tillåter nationella särregler.



Beslut i kommunstyrelsen den 23 augusti 2017 att Intraservice utvecklar en kommungemensam intern tjänst som tillhandahålls alla förvaltningar och bolag inom Göteborg Stad - dataskyddsenheten.

Enhetschef: Lise-Lotte Ringborg

DSO:

- Abtin Kronold (Jurist)
- Kiana Fanaey (Jurist)
- Johan Bergström (Arkivarie)
- Leopold Zainali (Jurist)
- Carina Seiberlich (Arkivarie)
- Nina Havner (Jurist)
- Martin Brunhage (Jurist)
- Patricia Gozon (Jurist)
- Alireza Haghighi (Ingenjör)

Tjänstebeskrivning DSO och tilldelningsbeslut är utskickade till förvaltningar och bolag (PuA)

Varför är det viktigt?

- En del av både privat och offentlig verksamhet.
- Berör oss alla även privat.
- Förändringar i samhället såsom digitalisering och ökning av online- tjänster har lett till att mängden personuppgifter som behandlas har ökat.

Vad är syftet med DSF?

”...skydda människor mot att deras personliga integritet kränks genom behandling av personuppgifter”.

Skapa enhetliga regler för hela EU.

Individernas rätt stärks.

DSF ska vara en integrerad del av bolagets arbetssätt.



- **Personuppgiftsansvarig (PuA)** – Den organisation t.ex. aktieföretag, stiftelse, förening eller myndighet som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till.
- **Personuppgiftsbiträde (PuB)** – Den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den ansvariges organisation.
- **Dataskyddsbud (DSO)** – Oberoende rådgivare för den personuppgiftsansvarige som kontrollerar att dataskyddsförordningen följs.
DSO omfattas av den sekretess som verksamheten har.
- **Dataskyddskontakt (DSK)** – Varje personuppgiftsansvarig organisation i Göteborg Stad ska ha minst en dataskyddskontakt. Dataskyddskontakten ska vara en kontaktperson till dataskyddsbudet och har som uppgift att kanalisera frågor från verksamheten till dataskyddsbudet.

Personuppgiftsansvarigas ansvar

- Omfattning
 - Ytterst ansvarig för all behandling.
 - Vidta lämpliga tekniska och organisatoriska åtgärder.
 - Kunna bevisa att behandlingen utförs korrekt inkl. åtgärdernas effektivitet.
- Fokus
 - Behandlingens art, omfattning, sammanhang och ändamål.
 - Riskerna med behandlingen.
 - Aktivt stödja dataskyddsombudets arbete.

DSO:s uppgifter

- Analysera och kontrollera huruvida bestämmelser om behandlingen efterlevs.
- Informera samt ge råd och utfärda rekommendationer till den personuppgiftsansvarige eller personuppgiftsbiträdet.
- Kontaktpunkt och samarbeta med tillsynsmyndigheten/DI.
- Rapporterar direkt till den personuppgiftsansvarige eller dennes högsta förvaltningsnivå
- Riskbaserat arbetssätt.

DSO:s ställning

Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

SKL kommentar:

Det är avgörande att ombudet involveras i tidigast möjliga skede av alla frågor där dataskydd blir aktuellt. Förutom att rådfrågas i samband med konsekvensbedömningar ska organisationen säkerställa att dataskyddsombudet till exempel:

- Regelbundet bjuds in till ledningsmöten på högsta beslutande och mellannivå,*
- Att ombudet närvarar vid beslut som påverkar dataskydd och att all relevant information görs tillgänglig i god tid,*
- Att ombudets bedömning alltid måste övervägas och om ombudets råd inte följs ska organisationen dokumentera skälen.*
- Att dataskyddsombudet kontaktas vid incidenter som kan medföra olovlig åtkomst av information.*

Ordning och reda på torpet – Ett register för personuppgiftsbehandlingar

- Alla företag och organisationer är i normalfallet skyldiga enligt förordningen att ha ett register över sina personuppgiftsbehandlingar. För varje behandling ska det bland annat framgå :
 - Vem som är internt ansvarig.
 - Vad syftet är med behandlingen.
 - Vilka typer av personuppgifter som behandlas.
 - Med vilken rättslig grund som personuppgifterna behandlas.

Nytt personuppgiftsregister

- Tilldelning har skett till Draftit Privacy AB.
- Implementeringsprojekt startar under hösten.



DSO:s iakttagelser/rapport avseende bolagets dataskyddsarbete

Avser perioden april – september 2018.

- Följsamhet utifrån tilldelningsanvisningar och DSF avseende organisation
 - DSK är utsedd och ersättare är anmäld.
 - DSO är anmäld till tillsynsmyndigheten/DI.
- Följsamhet utifrån bolagets informationsskyldighet och den registrerades rättigheter
 - Kommunikation och integritetspolicy på bolagets hemsida.
 - Bolaget tar hänsyn till DSF och integritetsfrågor t.ex. gällande beslutet om rökfritt boende, korrespondens med kund angående uppgifter som lämnas i samband med uppsägning och visning av en bostad.

Status inkomna ärenden – den registrerades rättigheter

Rätt till tillgång (utlämning av pu)	Rätt till radering	Rätt till rättelse	Rätt till data-portabilitet	Rätt till invändning	Rätt till begränsning
Antal: 1	Antal:	Antal:	Antal:	Antal:	Antal:

Forts. DSO:s iakttagelser/rapport avseende bolagets dataskyddsarbetet

- Följsamhet vid personuppgiftsincidenter som kan innebära risker för människors friheter och rättigheter
 - Bolaget rapporterar in och följer DSO:s råd och rekommendationer.
 - Fem personuppgiftsincidenter varav en är inrapporterad till Datainspektionen.
 - Bolaget känner igen en personuppgiftsincident.
 - Personalen vet hur och till vem personuppgiftsincidenter ska rapporteras.
 - Alla personuppgiftsincidenter dokumenteras.



Forts. DSO:s iakttagelser/rapport avseende bolagets dataskyddsarbete

- Kort beskrivning av inrapporterad personuppgiftsincident
 - "Phisingmail" den 18 juni 2018
- Avsaknad av tillräckliga rutiner för riskbedömning och incidenthantering mellan berörda PuA bolagen i koncernen och PuB/Framtidens IT samt deras underbiträde Microsoft.
- Identifierade brister gällande: tidsaspekt, relevant information och utförda åtgärder.

Resultat:

Kompletterad anmälan skickades till DI.

Bolaget har utsett en person och en koncerngemensam grupp som ansvarig att hantera personuppgiftsincidenter

Incidentrutiner inklusive information till de registrerade personerna togs fram.

Ännu okänt exakt mängd och kategori av personuppgifter som röjdes eller inte.

Inrapporterade åtgärder bör utvärderas.

DI beslut den 30 augusti 2018 – efter granskning avslutas ärendet utan ytterligare åtgärd.

Sammanfattningsvis iakttagelser och rekommendationer

- Bolaget har en etablerad dataskyddsorganisation förankrad i ledningen.
- Medvetenhet hos både beslutsfattare/PuA och medarbetare om DSF.
- Ett fortsatt aktivt engagemang och säkerställande av
 - organisatoriska resurser
 - utveckling av rutiner och riskanalyser
 - utbildningsinsatser

Rekommendation: DSF introduktionsinformation till alla nyanställda, riktade insatser till särskilda grupper i verksamheten, obligatorisk e-learning utbildning för all personal.

I syfte att DSF blir en integrerad del av bolagets arbetssätt.



Kontakt

**Dataskyddsenheten
Intraservice Ekonomi/ledning/styrning, Göteborgs Stad**

**Nina Havner
Dataskyddsombud
Mejl: nina.havner@intraservice.goteborg.se**

Tfn: 031-368 65 69