Hantering av personuppgifter och allmän informationssäkerhet

Varför?

Den digitala tidsåldern, med nya teknologier har inneburit att man samlar personuppgifter i allt större utsträckning.

Med GDPR antogs 2018 den mest omfattande privatlivslagstiftning till dagens datum – Allmänna dataskyddsförordningen. Lagstiftare och medborgare i Europeiska unionen (EU) har varit starkt skyddande för personuppgifter och integritet (PUL) i åratal, men med GDPR blir kraven ännu tuffare.

Lagen skyddar människors rätt till skydd av sina personuppgifter!

Vad räknas som personuppgifter?

Personuppgifter är all information som direkt eller indirekt kan knytas till en person. Typiska personuppgifter är personnummer, namn och adress. Även foton på personer klassas som personuppgifter. Med andra ord menas all information som på något sätt kan identifiera vilken person det handlar om.

Största vikt ligger på s.k. känsliga personuppgifter. Med känsliga personuppgifter menas t ex en persons sexuella läggning, religion, politiska åsikt och etniska ursprung. Till känsliga personuppgifter räknas även hälsouppgifter om personen och uppgifter om vilken fackförening personen tillhör. Även personnummer räknas som extra skyddsvärt.

Vem gäller det?

Detta gäller alla som på något sätt hanterar personuppgifter i sitt arbete.

Är du chef så ansvarar du för att informera dina medarbetare om vad som gäller.
Är du medarbetare så är du skyldig att följa dessa regler.

Vad innebär det rent praktiskt?

Vi måste ha koll på var vi sparar personuppgifter, varför och hur vi sköter om dem!

Rensa – Vi måste rensa personuppgifter vi inte har grund att lagra*
Uppdatera – De uppgifter vi har lagrade måste vara aktuella och korrekta
Registerförteckningar – Vi måste veta var vi lagrar personuppgifter
Registerutdrag – Vi måste kunna ta fram var en person förekommer
Rapportera – Om något går fel måste det rapporteras
Personuppgiftbiträdesavtal – För att en extern part ska få behandla data vi samlat in krävs avtal

* Viktigt! Innan ni rensar personuppgifter måste ni först kontrollera vad som måste sparas enligt lag och för att ni ska kunna utföra ert arbete.

Om något går snett

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har:

blivit förstörda
gått förlorade på annat sätt
kommit i orätta händer

Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter. Incidenter ska rapporteras så snart de upptäcks. I första hand till personuppgiftssamordnare och i dennes frånvaro i andra hand till SOC IT-team via e-tjänsten SOC Ärenden IT-team, välj kategori incidentrapportering GDPR.

https://insidan.it.pitea.se/grupper/socialforvaltningen/it-stod/
E-tjänsten ligger under avsnittet för länkar.

Läsvärt

Det finns bra information att hämta både på insidan och hos Integritetsskyddsmyndigheten - IMY (tidigare Datainspektionen).

https://insidan.it.pitea.se/stod-i-arbetet/dataskyddsforordningen-gdpr/
https://www.datainspektionen.se/lagar--regler/dataskyddsforordningen/
eller www.imy.se

Goda råd till dig som medarbetare

- Samla inte på dig nya personuppgifter i onödan, måste ha laglig grund till att spara.
- Kom överens med dina kollegor var ni sparar viktig information och spara inte dubbelt.
- E-post är inte ett säkert media var därför sparsam med att skicka personuppgifter via e-post. Känsliga personuppgifter får inte skickas via e-post.
- Se till att städa bort inaktuella uppgifter och data som inte måste sparas.
- Lämna inte ifrån dig personuppgifter till någon extern part om ni inte har tydliga rutiner för detta.
- Tänk på att T: och din e-post är personlig, men inte privat.

DISA - datorstödd informationssäkerhetsutbildning för användare

DISA är en webbaserad kurs som kommunen starkt rekommenderar samtliga anställda att genomgå. Utbildningen hittar du här (men kräver att du har fått ditt kommunkonto först).

Syftet med kursen är att skapa medvetenhet och kännedom kring informationssäkerhet - dels för att veta vad du bör undvika, dels för att veta hur du bör agera om olyckan är framme.

Om du inte har möjlighet att gå kursen redan nu kan du här läsa om de mest grundläggande delarna i informationssäkerhet som alla anställda inom Socialtjänsten måste känna till som utgår från DISA.

Varför är informationssäkerhet viktigt?

Vi behöver skydda vår information så att den inte manipuleras, är tillgänglig och så att endast personer med behörighet har tillgång till den.

Säkert beteende

Allt som ligger framme på ditt skrivbord är ofta inte önskvärt att andra personer ser eller läser. Är det ett samtal med känsliga uppgifter är det viktigt att ingen utomstående kan höra vad som sägs.

Lösenord

Skriv inte ner lösenord på en minneslapp, använd inte lösenord med en personlig anknytning och se till att ditt lösenord är din hemlighet, inte arbetsplatsens gemensamma. Om någon använder din inloggning kan du bli ansvarig för något de gör på datorn.

E-post

Tänk på att du ansvarar för det material som du arbetar med, oavsett var du gör det. Betrakta det som du skickar via e-post som att du skickar ett vanligt vykort, det vill säga det skickas helt öppet och kan komma att läsas av obehöriga.

Skadlig kod

Man riskerar att drabbas av skadlig kod när man öppnar okända bilagor i e-post, surfar på Internet eller importerar filer till sin dator via olika media. Så snart du märker att du har drabbats bör du lämna datorn till din IT-support. Ge inte ut mer information än nödvändigt om dig själv, klicka inte på länkar som du inte vet vad de innehåller och kommunicera som grundregel bara med personer som du känner eller vet vilka de är. Mer information från centrala IT-avdelningen hittar du här (när du har ett kommunkonto).

Sociala medier

Rent allmänt bör du hantera sociala medier på Internet på samma sätt som du skulle göra om du umgicks med personer i verkliga livet. Det finns en mängd olika brott i lagstiftningen som kan ge kännbara straff med anledning av vad som skrivs på nätet. Både organisationer och enskilda har ett ansvar för vad de själva publicerar.

Mobila enheter

Tänk på att inte lämna dina enheter utan uppsikt, låna inte ut dem och undvik att använda dem till privata ändamål. När du arbetar med dem i publika miljöer, utgå ifrån att obehöriga inte ska kunna se vad du arbetar med, oavsett materialets känslighet. Tänk på att trafiken i öppna wifi-nätverk oftast går att avlyssna.

Molntjänster

Kom ihåg att i många fall innebär lagring i molnet att du inte vet var eller med vilken säkerhet informationen hanteras. Se till att du har kunskap om vad som gäller för olika typer av molnbaserade lösningar t ex. MS 365.

Säkerhetskopiering

Förvara alltid dina säkerhetskopior på ett säkert ställe. En huvudregel kan vara att backup ska förvaras minst lika säkert som de ordinarie uppgifterna, fast på en annan plats.

Loggning och spårbarhet

Spårbarhet innebär att man genom loggning kan identifiera och följa förloppet för olika händelser som skett på datorn. Syftet är att finna vem som är skyldig till ett intrång eller en säkerhetsrelaterad incident.

Källa: https://www.informationssakerhet.se/kompetensutveckling/msbs-webbutbildning-disa/