Datum: 2024-09-17
Dokumentansvarig: Dataskyddskontakt

Stödjande dokument – hantering av personuppgifter på lagringsytor

Syftet med dokumentet

När du till exempel skriver eller tar emot ett mejl eller sparar personuppgifter på en lagringsyta utanför verksamhetssystemen, behöver du förhålla dig till principerna inom dataskyddsförordningen (GDPR) om vad som är en korrekt behandling av personuppgifter. I detta dokument får du stöd i hur du ska hantera personuppgifter och sekretessmarkerad information utanför verksamhetssystemen.

För råd och tips på hur du skickar och tar emot krypterad e-post, se kunskapsportalen för Microsoft 365 här: Kryptera e-postmeddelanden med känsligt innehåll (sharepoint.com)

Se även styrande dokument:

- Göteborgs Stads regler för användande av epost
- Dokumenthanteringsplanen

Begreppslista

Definitionerna av begreppen är hämtade från tillsynsmyndigheten för dataskyddsfrågor, Integritetsskyddsmyndigheten (IMY).

Begrepp	Definition
Behandling (av personuppgifter)	Behandling är ett vidsträckt begrepp och innefattar allt som kan göras med personuppgifter. Till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning, blockering, utplåning eller förstöring av personuppgifter.
Känsliga personuppgifter	Personuppgifter som till exempel avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.
Personuppgift	All slags information som direkt eller indirekt kan knytas till en (fysisk) person som är i livet. Även bild- och ljuduppgifter om en (fysisk) person räknas som

	personuppgifter, även om inga namn nämns. Krypterade eller kodade uppgifter är också personuppgifter om någon har en nyckel som kan koppla dem till en person.
Personuppgiftsansvarig	Personuppgiftsansvarig är den organisation (till exempel aktiebolag, stiftelse, förening eller myndighet) som bestämmer för vilka ändamål som uppgifterna ska behandlas och hur behandlingen ska gå till. Det är alltså inte chefen på en arbetsplats eller en anställd som är personuppgiftsansvarig. Även en fysisk person kan vara personuppgiftsansvarig vilket till exempel är fallet för enskilda firmor. (För hanteringen av personuppgifter i förvaltningen för funktionsstöd är Nämnden för funktionsstöd ytterst personuppgiftsansvarig.)
Registrerad	Den som en personuppgift avser, det vill säga handlar om.

Inledning

All behandling av personuppgifter måste följa de grundläggande principerna som anges i dataskyddsförordningen. Dessa grundläggande principer definieras i artikel 5 i dataskyddsförordningen och innebär bland annat att du endast ska behandla personuppgifter som är nödvändiga för att utföra dina arbetsuppgifter och att personuppgifterna ska behandlas på ett säkert sätt.

När du hanterar personuppgifter är det därför viktigt att:

- uppgifterna behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade
- inte behandla fler personuppgifter än vad som behövs
- se till att personuppgifterna är riktiga och uppdaterade
- radera personuppgifterna när de inte längre behövs (se dokumenthanteringsplanen)
- skydda personuppgifterna så att inte obehöriga får tillgång till dem och så att de inte förloras eller förstörs

Klassning av information

Informationsklassning innebär att man värderar information utifrån vilka konsekvenser det får om förvaltningen inte har tillräckligt skydd för informationens konfidentialitet, riktighet och tillgänglighet. Genom att klassa informationen så tar man ställning till:

- Vad kan konsekvenserna bli om informationen kommer obehöriga till del (konfidentialitet)?
- Vad kan konsekvenserna bli om informationen är manipulerad eller förstörd (riktighet)?
- Vad kan konsekvenserna bli om någon (som är behörig) inte får tillgång till informationen (tillgänglighet)?

I tabellen nedan kan du se vilken klassning olika typer av information har inom förvaltningen.

Informationstyp ***Klass 3 information kan i vissa fall vara:***	**Beskrivning av konsekvensen om informationen inte skyddas**	**Klassning**
Skyddade och känsliga personuppgifter Sekretessklassade uppgifter enligt OSL Patientdata som till exempel ordination	**Konfidentialitet:** Obehörig åtkomst medför mycket allvarlig skada för verksamheten och mycket allvarlig negativ påverkan på enskild individs rättigheter. **Tillgänglighet:** Verksamheterna har stora svårigheter att fullgöra en eller flera av sina primära uppgifter om informationen i IT-systemet är otillgänglig. Mycket allvarlig negativ påverkan på enskild individs rättigheter eller hälsa. **Riktighet:** Oriktig, ofullständig information i systemet medför omfattande skada för verksamheten och mycket allvarlig negativ påverkan på enskild individs rättigheter eller hälsa.	**Klass 3**
Klass 2 information kan i vissa fall vara: Personuppgifter (ej känsliga eller skyddade, vilket är klass 3) Sekretessklassade uppgifter enligt OSL	**Konfidentialitet:** Obehörig åtkomst medför betydande skada för verksamheten och betydande negativ påverkan på den enskildes rättigheter. **Tillgänglighet:** om informationen i IT-systemet är otillgänglig kan det innebära att verksamheterna kan fullfölja primära uppgifter men med kraftigt påverkad effektivitet med betydande negativ påverkan på den enskildes rättigheter eller hälsa. **Riktighet:** Oriktig, ofullständig information i systemet medför betydande skada för verksamheten och betydande negativ påverkan på	**Klass 2**

	den enskildes rättigheter eller hälsa.	
Klass 1 information kan i vissa fall vara: Arbetshandlingar Information avsedd för internt bruk Allmänna offentliga handlingar Uppgifter som inte är skyddsvärd och innehåller enstaka enskilda personuppgifter av ej känslig karaktär	**Konfidentialitet:** Obehörig åtkomst medför måttlig skada för verksamheten och enskilda. **Tillgänglighet:** innebär att verksamheterna kan fullfölja primära uppgifter men med något reducerad effektivitet. Kan få en begränsad negativ påverkan på den enskildes rättigheter eller hälsa. **Riktighet:** Oriktig information medför betydande skada för verksamheten och betydande negativ påverkan på den enskildes rättigheter eller hälsa.	**Klass 1** **Detta kallas även Grundläggande skyddsnivå**
	Konfidentialitet: Obehörig åtkomst medför ingen skada för verksamheten eller enskild. **Tillgänglighet:** information där förlust av tillgänglighet inte medför negativ skada för verksamheten eller enskild. **Riktighet:** information där förlust av riktighet inte medför negativ skada för verksamheten eller enskild.	**Ingen skyddsnivå**

Var kan information lagras?

Verksamhetssystem

Informationen ska i första hand alltid förvaras i verksamhetssystem. Majoriteten av allt vi lagrar kring brukare, anhöriga, anställda med flera ska finnas i dessa system. Exempel på verksamhetssystem är Treserva, Personec, Proceedo, etc.

SharePoint/Forms/Teams/OneDrive/OneNote/Outlook

Vid hantering av information som inte kan lagras i verksamhetssystemen ska SharePoint användas. ***Undantaget är känslig eller sekretessbelagd information (klass 3 och i vissa***

fall klass 2 information i tabellen ovan) – detta ska inte lagras i SharePoint, Forms, Teams, OneDrive, OneNote eller Outlook. Sådan information måste uteslutas eller omformuleras innan den kan lagras där.

I:mapp och H:mapp

Om det inte finns möjlighet att spara känslig eller sekretessinformation i något av Göteborgs Stads verksamhetssystem så ska informationen sparas på en I-mapp specifikt för detta ändamål, alternativt i din Hemkatalog. (H:mapp)

I tabellen nedan kan du se vilken skyddsnivå de olika lagringsytorna har. Det innebär att informationen som hanteras där inte får ha en högre klassning än den som visas.

Yta	**Vilken information kan hanteras/läggas på ytan?**	**Ytterst ansvarig för ytan**	**Vad kan du göra?**
Verksamhetssystem	Klass 3 information. OM systemet är klassat för att klara lagring av klass 3 information För skyddade personuppgifter ska det finnas särskilda behörighetsstrukturer	Chef.	Hantera i så stor utsträckning som möjligt all din information inom verksamhetssystemen. Om du behöver hämta ut information från systemet ska detta hanteras på ett säkert sätt. I de fall där dessa system kan användas för kommunikation ska det användas. Ett exempel är meddelarfunktionen i Treserva.
Teams	Klass 2 information. Teams ska inte användas för känslig eller sekretessbelagd information.	Utpekad informations-ansvarig ansvarar för ytan och övergripande innehåll.	Här kan du kommunicera med andra i chatt och i inlägg i olika kanaler. Filer lagras i SharePoint, men kan presenteras för alla medlemmar i Teams. Alla filer som hanteras i Teams finns lagrade i SharePoint. Text i inlägg och olika chattar kan endast tas bort av dig själv. Chatthistorik raderas automatiskt efter tre månader.

			Teams är ett kommunikationsverktyg, inte en lagringsyta, även om du når lagringsytan i SharePoint via Teams.
SharePoint	Klass 2 information. SharePoint ska inte användas till känslig eller sekretessbelagd information.	Utpekad informations-ansvarig ansvarar för ytan och övergripande innehåll.	Här kan du skapa och lagra filer som automatiskt delas med alla medlemmar i ytan. Rensa och kasta arbetsmaterial som inte längre behövs fortlöpande. Filer finns kvar på ytan även om du slutar.
OneDrive	Klass 2 information OneDrive ska inte användas till känslig eller sekretessbelagd information.	Du själv ansvarar.	Här kan du skapa och lagra filer exempelvis egna mallar, lathundar, referensmaterial eller arbetsmaterial. Du kan dela filer med kollegor i staden och låta dem redigera i filen. Rensa och kasta arbetsmaterial fortlöpande som inte längre behövs.
Outlook	Klass 2 information. Outlook ska inte användas till känslig eller sekretessbelagd information.	Du själv ansvarar.	Öppnas dagligen, rensas fortlöpande och bevakas så att inkomna handlingar hanteras på rätt sätt och förs över till verksamhetssystem. Känsliga personuppgifter eller sekretessuppgifter överförs direkt till godkänt verksamhetssystem och tas därefter bort. Information av ringa betydelse kastas direkt, även om den innehåller sekretess, exempelvis en kollega skriver att hen är sjuk. Ska inte innehålla mail som är äldre än 2 år.

OneNote	Klass 2 information. OneNote ska inte användas till känslig eller sekretessbelagd information.	Eget ansvar för den personliga anteckningsboken. Övriga böcker som delas med flera ansvarar chef för.	Används för att skapa anteckningar, antingen dina egna eller delade med andra, till exempel mötesanteckningar. Rensa löpande och kasta arbetsmaterial som inte längre behövs. Den personliga anteckningsboken försvinner 30 dagar efter avslutad anställning. Vissa mötesanteckningar ska bevaras enligt dokumenthanteringsplanen, andra kan gallras 2 år efter upprättande. Se dokumenthanteringsplanen för mer information.
Lotus Notes (LIS)	Klass 3 information. Känslig och sekretessbelagd information kan hanteras i mappar med begränsad behörighet. Skyddade personuppgifter ska inte läggas i LIS	Utpekad informationsansvarig ansvarar för databasen och övergripande innehåll.	Används för förvaltningens handlingar inklusive nämnd- och utskottshandlingar (blå-pluppade mappar/dokument). Notes kommer avvecklas och ersättas av nytt system. Inga nya databaser kommer att skapas i förvaltningen.
Funktionsstöd Data (I:)	Klass 3 information. Här kan du lagra känslig information, som alla användare med tillgång till mappen behöver ta del av, som inte kan förvaras i verksamhetssystem.	Utpekad informationsansvarig ansvarar för ytan och övergripande innehåll.	Här kan du skapa och lagra filer som automatiskt delas med alla medlemmar som är behöriga i mappen. Rensa löpande och kasta arbetsmaterial som inte längre behövs. Tänk på att följa instruktionen som följer med beställningen av mappen.

			Allt som finns i mappen är tillgängligt för alla de som är behöriga till mappen.
Hemkatalog (H:)	Används för att skapa och lagra personliga arbetsfiler. Här kan du lagra känslig information, som endast du behöver ta del av, som inte kan förvaras i verksamhetssystem.	Du själv.	Här kan du lagra alla dina filer som inte ska föras in i ett verksamhetssystem. När du avslutar din anställning tas Hemkatalogen (H:) bort och innehållet försvinner.

Konkreta tips

Som utgångspunkt gäller att känslig information och personuppgifter endast ska hanteras i verksamhetssystem.

Använd ärendenummer (som också är en personuppgift) i stället för andra mer specifika personuppgifter som kan vara mer direkt utpekande. Du minimerar då risken för att en person blir identifierad. Kan du till exempel använda initialer i stället för ett fullt namn? Kan du använda födelseår eller födelseår och månad i stället för ett helt personnummer?

Ärendenummer kan användas i din Outlookkalender och i ärenderaden för ett mejl om inga andra uppgifter samtidigt skrivs in om ärendet så som ”avslutandesamtal”, ett namn eller annan uppgift om ärendet. I

Inga direkta personuppgifter eller känslig information får förekomma i ämnesraden på de mejl du skickar.

Personuppgifterna ska skyddas så inte obehöriga kan ta del av dem. Finns det en behörighetsbegränsning för den lagringsyta du sparar informationen på?

Om du behöver hantera känsliga personuppgifter utanför verksamhetssystemet, för att kunna utföra dina arbetsuppgifter, använd I:mapp med begränsade behörigheter.