region västerbotten

Utgåva nr: 2.0
Giltigt fr.o.m. 2023-02-22
Giltigt t.o.m. 2025-02-23

**Riktlinje**
Fastställt av: Magdalen Alatalo Berg
Upprättat av: Sara Salberg
Granskare: Elena Collin
Organisation gäller inom: Region Västerbotten

# Digital informationshantering

## Förändringar från föregående utgåva
Förtydligande kring begreppet skyddsvärd information, tillägg kring ChatGPT och liknande samt delning av information via Platina.

## Omfattning
Riktlinjen omfattar hela myndigheten Region Västerbotten och riktar sig mot all personal som arbetar för Region Västerbotten vid hantering av digital information.

## Bakgrund
Denna riktlinje föreskriver hur digital information ska hanteras inom Region Västerbotten. Den ökade digitaliseringen och att informationsflöden i högre grad sker via digitala hjälpmedel gör att det finns ett behov av att ha en riktlinje för den digitala informationshanteringen för att säkerställa korrekt hantering.

## Syfte
Syftet med riktlinjen är att säkerställa att Region Västerbotten hanterar information på ett sätt som är lagligt, informationssäkert, cybersäkerhet och som säkerställer bevarande av allmänna handlingar.

## Lagar och andra krav
De lagar som styr hur Region Västerbotten ska hantera sin information är:
- Dataskyddsförordningen (2016/679)
- Arkivlagen (SFS 1990:782)
- Offentlighets och sekretesslagen (SFS 2009:400)
- Patientdatalagen (SFS 2008:355)
- Tryckfrihetsförordningen (1945:105)
- Lag om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1174)
- Förordning om informationssäkerhet för samhällsviktiga och digitala tjänster (SFS 2018:1175)
- Socialstyrelses föreskrifter och allmänna råd om journalföring och behandling av personuppgifter i hälso- och sjukvården (HSLF-FS 2016:40)

## Ansvar och befogenheter
*Enskild anställd*:
- Ansvarig för att det arbetssätt man själv tillämpar följer riktlinjerna.

*Verksamhetschef:*
- Ansvarig för att de arbetssätt som finns på enheten följer riktlinjerna för informationshantering.
- Ansvarig för att se till att alla anställda känner till riktlinjer och utbildas om att arbeta informationssäkert.
- Ansvarig för att se till att det finns en dokumenthanteringsplan där det framgår hur olika typer av dokument ska hanteras.
- Informationsägare för den information som skapas och används inom verksamheten. Hälso-

och sjukvårdsförvaltningen har även en övergripande informationsägare. För beskrivning se Informationsägarskap i Hälso- och sjukvården

*Arkivarie:*

- Råd och stöd vid dokumenthantering.

*Informationssäkerhetssamordnare:*

- Ansvarar för att driva och samordna det Region Västerbotten gemensamma informationssäkerhetsarbetet.

*Dataskyddsombud:*

- Ansvarar för att övervaka att organisationen följer dataskyddsförordningen.

## Beskrivning/Genomförande

**Definitioner**

*Känslig information*
Känslig information kan antingen vara känsliga personuppgifter eller uppgifter som på något sätt skyddas av sekretess, t.ex. upphandlingssekretess, företagshemligheter, patientuppgifter eller uppgifter om anställda.

*Personuppgifter*
Personuppgifter är alla uppgifter som direkt eller indirekt kan identifiera en person, till exempel namn, personnummer, bilder, registreringsnummer.

*Känslig personuppgift*
Med känsliga personuppgifter menar man bland annat uppgifter om 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.

*Skyddsvärd information*
Skyddsvärd information är sådan information som vi varken vill förlora eller låta andra ta del av. Det kan handla om känsliga uppgifter, sekretess men också annan typ av information som kan skada verksamheten om den kommer i orätta händer. Det kan till exempel handla om information om patienter, riskanalyser eller uppföljningsresultat som visar på sårbarheter inom verksamheten, kod som beskriver hur våra system är uppbyggda, eller beskrivningar över vart skyddsvärd utrustning finns placerad, med mera.
Det finns personuppgifter som inte hör till kategorin känsliga personuppgifter, men som ändå är extra skyddsvärda och ska hanteras som skyddsvärd information. Sådana typer av uppgifter är till exempel personnummer, löneuppgifter, värderande uppgifter (till exempel uppgifter från utvecklingssamtal, resultat från personlighetstester eller personlighetsprofiler), information som rör någons privata sfär och uppgifter om sociala förhållanden.

Skyddsvärd information handlar alltså om sådan typ av information som potentiellt kan skada enskilda personer eller verksamheten ifall den kommer i orätta händer, och ska skyddas.

*Allmän handling*
En allmän handling är en handling som förvaras hos en myndighet och som enligt Tryckfrihetsförordningen kan anses vara antingen inkommen eller upprättad. Att en handling är allmän ska inte förväxlas med att den är offentlig, då en allmän handling kan vara sekretessbelagd. Alla har rätt att ta del av allmänna handlingar så länge de inte är sekretessbelagda, om förfrågan att ta del av sekretessbelagd handling inkommer ska alltid en sekretessprövning göras. Några exempel

på allmänhandling är journaler, protokoll, korrespondens (till exempel e-mejl och brev) och informationsmaterial internt och externt, med mera.

*Diarieföring*
Diarieföring innebär att registrera allmänna handlingar i ett diarium. Mer om diarieföring finns i det styrande dokumentet *"Diarieföring av allmänna handlingar*" i ledningssystemet.

*Journalföring*
Hälso- och sjukvården har skyldighet att föra journal på sina patienter. Journal ska föras i avsett journalsystem.

**Beskrivning**
Känslig information som information om patienter, ekonomisk information och personalinformation ska enbart hanteras i de system som är avsedda för hantering av dessa uppgifter. Exempelvis journalsystem, HR-system och ekonomisystem. Finns det behov som inte dedikerade system kan tillgodose görs ett ärende i behovssystemet. Delning av information utanför dessa system får endast ske enligt riktlinje.

Personuppgifter, även de som inte är känsliga, får bara hanteras om det finns en laglig grund för att hantera dessa. Varje personuppgiftsbehandling måste även följa hela GDPR:s regelverk, till exempel att personerna ska få information om personuppgiftsbehandlingen, så lite uppgifter som möjligt ska sparas och det ska bestämmas hur länge uppgifterna ska sparas. Myndigheten ska alltså inte hantera personuppgifter som inte krävs för att utföra sina uppgifter.

Alla personuppgiftsbehandlingar som förs till exempel. i Platina och på V: och G: ska förtecknas i enhetens personuppgiftsregister av verksamheterna själva. Stöd för registerförteckning hittas i SharePoint via följande länk: https://vlladmin.sharepoint.com/sites/app-reg-gdpr
Tröskelanalys ska också göras för att bedöma om en konsekvensbedömning ska göras. Rutin för tröskelanalys finns hittas i ledningssystemet "*Tröskelanalys avseende dataskydd*". Skulle tröskelanalysen visa att en konsekvensbedömning behöver genomföras ska det också genomföras. Rutin för Konsekvensbedömning avseende dataskydd hittas också i ledningssystemet.

Informationssäkerhetsklassning handlar om att värdera information utifrån aspekterna tillgänglighet, konfidentialitet och riktighet. Teknikkomponenter med tillhörande informationstillgångar ska informationssäkerhetsklassas med målet att informationen ska hanteras på rätt sätt och få rätt skydd. För mer detaljerad beskrivning av de olika aktiviteterna kopplat till informationssäkerhet i processen för anskaffning, förändring och utveckling av informationssystem, se separat rutin för det.

*Lagringsytor och vad de ska användas till*:

- **Platina** – Platina är i första hand ett ärende och dokumenthanteringssystem, men kan också användas för information som inte har ett avsett system. Även dokument som innehåller känsliga personuppgifter och annan känslig/skyddsvärd information kan förvaras i åtkomstbegränsade arbetsytor. Ägare av dokumentplatsen hanterar själv behörigheterna dit och det är endast de som har behörighet som kan ta del av informationen där. Arbetsytor för samarbete kring känsliga personuppgifter kan skapas i Platina. Platina kan med fördel användas då det finns en koppling till diariet, allmänna handlingar ska alltid diarieföras.
- **Lokal Lagrings yta V**: Finns både samarbetsytor som är till för tillfälliga samarbeten och enhetentsytor i utforskaren. Ett system för information som inte har ett avsett system. Även dokument som innehåller känsliga personuppgifter eller annan skyddsvärd information kan

förvaras på åtkomstbegränsade arbetsytor. Den specifika enhetsmappen har alla på ens enhet/avdelning tillgång till, notera att bedömning behöver göras om specifik information är avsedda för alla inom enheten. Vidare så kan chef på organisationsenhet begära ytor med snävare access.

- **Teams, OneDrive, Outlook, SharePoint och övriga molnbaserade Microsoft Office system samt ChatGPT, Bard eller andra LLM-modeller**– Inga känsliga personuppgifter, sekretess och annan skyddsvärd information får förekomma här. Att hantera personuppgifter i dessa system är olagligt då det automatiskt innebär tredjelandsöverföring vilket strider mot GDPR. Att dela övrig sekretess i dessa system strider mot OSL, då sekretessbelagda uppgifter i dessa system kan anses vara röjda.

  *Teams* kan användas för intern kommunikation inom en verksamhet eller ett arbetsområde. *Outlook* används för mejl och kalenderbokning. *SharePoint* är en dokumentlagringsyta och kan användas för verksamhetsinformation som inte är av skyddsvärd karaktär.

*Delning av information*

Muntlig överföring av känslig information är inte tillåtet via Microsoft Teams, av samma anledning att Microsoft Office-system inte lämpar sig för förvaring av känslig information. Känslig information delas via telefonsamtal, eller via säker videokonferens. Om känsliga personuppgifter ska diskuteras i ett Teams-möte ska personerna som diskuteras avidentifieras.

Vid delning av känslig information via e-mejl ska tjänsten Cryptshare användas, vilket möjliggör att informationen i meddelandet stannar inom Region Västerbottens servrar. Delning av krypteringsnyckeln får inte ske via e-mejl, den ska delas via telefon eller sms. För mer information om Cryptshare se sidan Säker e-post på intranätet.

Platina kan också användas för att dela känslig information med specifika personer, då dokument åtkomst kan begränsas, både genom att skicka till specifika personer via Platina eller delas på åtkomstbegränsade arbetsytor.

*Vilken information ska förvaras var?*

När en ska avgöra vilken information som ska sparas var behöver hänsyn tas till vilka lagringsytor som lämpar sig för att förvara informationen. Det är också viktigt att hålla sin information ordnad och strukturerad. Det ska vara enkelt att hitta informationen. Det kan därför vara bra att besluta sig för en förvaringsplats för viss information. Informationen ska också hanteras på det sätt som gällande dokumenthanteringsplan föreskriver.

Dokumenttyper som det ofta förekommer frågor om:

- Styrande dokument och blankettmallar ska förvaras i Ledningssystemet
- Protokoll från APT, ledningsgrupp och andra protokoll - förvaras på enhetens Platina-plattform eller på enhetsyta på V:, och i vissa fall i Microsoft 365 verktyg, exempelvis OneNote, eller enhetsyta i Sharepoint. Förvaring i Office 365 verktyg får bara ske om det inte finns känsliga personuppgifter i dokumentet, som till exempel facklig tillhörighet.
- Minnesanteckningar – ska inte förväxlas med ett protokoll. En minnesanteckning får inte innehålla beslut eller annat av vikt för ett ärende, då är det ett protokoll. Minnesanteckningar förs för den egna anställdas skull och som inte innehåller information av vikt för något ärende kan gallras, då de är ett arbetsmaterial.

## Dokumentation och arkivering

Ej tillämpbar.

## Historik
Ej tillämpbar.

## Utarbetat av
Objektet ärende- och dokumenthantering
Arkivarie och Informationssäkerhetssamordnare, med hjälp av kompetens inom bland annat juridik och IT.

## Referenser
Anskaffning, förändring och utveckling av informationssystem
Tröskelanalys avseende dataskydd (Dokumentnr: 74382)
Konsekvensbedömning avseende dataskydd (Dokumentnr: 65917)
Informationsägarskap i hälso- och sjukvården (Dokumentnr: 74124)
Diarieföring av allmänna handlingar (Dokumentnr: 165680)
Sida från Intranätet om säker epost
Stöd för registerförteckning: https://vlladmin.sharepoint.com/sites/app-reg-gdpr