

## 2024 år granskningsrapport av behandling av personuppgifter i Överförmyndarnämndens register som inte behandlas automatiskt enligt den Europeiska Dataskyddsförordningen (GDPR)

Fastställd av Överförmyndarnämnden  
Framtagen av Regionens dataskyddsombud  
Datum 2024-10-29  
Gäller  
Ärendenr ÖFN 2024/8  
Version 1.0

Överförmyndarnämnden  
Region Gotland

### Innehåll

#### Sammanfattning

Överförmyndarnämndens behandling av personuppgifter i fysiska register uppfyller GDPR's krav på teknisk och administrativ säkerhet vid behandling av register som inte förs automatiskt, med undantag för säkerheten vid förvaring av äldre handlingar. Förvaltningens behandling av personuppgifter i register som inte förs automatiskt utgör en stor del av verksamheten och omfattar personuppgifter med högt skyddsvärde men avser ett begränsat antal registrerade. Det är ett fåtal personer som har åtkomst till uppgifterna i lokaler där säkerheten är anpassad efter uppgifternas skyddsvärde, men äldre handlingar har tidigare förvaras i ett delat arkiv vilket inte är lämpligt, men detta har åtgärdats.

## Bakgrund

Reglerna i GDPR omfattar såväl digitala som annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Inom regionens verksamhet kan de flesta skrifter utom temporära etiketter (t.ex. på beställningar av speciella måltider) anses vara avsedda att ingå i ett register, med följd att det är en relativt stor mängd personuppgifter som inte behandlas automatiskt. Dataskyddsombudet har som en del av uppdraget genomfört en granskningsaktivitet där efterföljanden av artiklarna 5 (behandlingen och ansvarsskyldigheten), 24 (lämpliga strategier för dataskydd), 25 (dataskydd) och 32 (lämplig säkerhet), granskas avseende de register för personuppgiftsbehandling som inte är automatiserade. Tidigare genomförda granskningar av säkerhet för behandlingarna har huvudsakligen avsett den digitala behandlingen, men då det förekommer behandling av personuppgifter även i andra automatisk förda register finns ett behov av att verifiera säkerheten även för detta. I de flesta av nämndens verksamheter finns en tydlighet kring och genomförande av "digitala original", men det finns några undantag där detta inte är helt tydligt (t.ex. antagningshandlingar, betygsregister). Det kan befaras att ökade krav på resiliens och återställande kan leda till en ökad betydelse av behandling av personuppgifter i fysiska handlingar.

Innan den omfattande digitaliseringen var fysiska handlingar det huvudsakliga sättet att behandla personuppgifter, vilket innebär att det finns kunskap och rutiner för hanteringen även om de rutinerna kanske inte motsvarar GDPR's krav samtidigt som det nu är mindre fokus än tidigare på fysiska handlingar.

I grunden ställs samma krav på säkerheten för personuppgifter i ett fysiskt register som det gör på ett digitalt, t.ex. avseende dataminimering, styrning, behörigheter och åtkomstkontroll. En klassning av handlingar ska således innebära ett motsvarande skydd för de fysiska uppgifterna.

I och med att artikel 5 innefattar den s.k. ansvarsskyldigheten är det viktigt att regionen kan visa upp inte bara att utan även hur skyldigheten fullgörs. Brister i uppfyllnad av Artiklarna 24, 25 och 32 är en vanlig grund för sanktionsavgifter inom EU. I och med ansvarsskyldigheten krävs kontinuerliga uppdateringar och justeringar utifrån omvärldshändelser för att lämplig säkerhet ska kunna anses vara uppfylld i enlighet med art 24 p1. När ny teknik eller metoder introduceras, såsom vid byte av leverantör eller vid förändring av vilka uppgifter som behandlas, eller då nya hot uppkommer behöver det regelbundet prövas och verifieras att den tekniska och administrativa säkerheten är lämplig.

### **Artikel 5 Principer för behandling av personuppgifter**

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller

skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).

2. Den personuppgiftsansvarige ska ansvara för och kunna visa att punkt 1 efterlevs (ansvarsskyldighet).

#### **Artikel 24 Den personuppgiftsansvariges ansvar**

1. Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med denna förordning. Dessa åtgärder ska ses över och uppdateras vid behov.

2. Om det står i proportion till behandlingen, ska de åtgärder som avses i punkt 1 omfatta den personuppgiftsansvariges genomförande av lämpliga strategier för dataskydd.

3. Tillämpningen av godkända uppförandekoder som avses i artikel 40 eller godkända certifieringsmekanismer som avses i artikel 42 får användas för att visa att den personuppgiftsansvarige fullgör sina skyldigheter. 4.5.2016 L 119/47 Europeiska unionens officiella tidning SV

#### **Artikel 25 Inbyggt dataskydd och dataskydd som standard**

1. Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas.

2. Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

3. En godkänd certifieringsmekanism i enlighet med artikel 42 får användas för att visa att kraven i punkterna 1 och 2 i den här artikeln följs.

### **Artikel 32 Säkerhet i samband med behandlingen**

1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt

a) pseudonymisering och kryptering av personuppgifter,

b) förmågan att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna,

c) förmågan att återställa tillgängligheten och tillgången till personuppgifter i rimlig tid vid en fysisk eller teknisk incident,

d) ett förfarande för att regelbundet testa, undersöka och utvärdera effektiviteten hos de tekniska och organisatoriska åtgärder som ska säkerställa behandlingens säkerhet.

2. Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

3. Anslutning till en godkänd uppförandekod som avses i artikel 40 eller en godkänd certifieringsmekanism som avses i artikel 42 får användas för att visa att kraven i punkt 1 i den här artikeln följs.

4. Den personuppgiftsansvarige och personuppgiftsbiträdet ska vidta åtgärder för att säkerställa att varje fysisk person som utför arbete under den personuppgiftsansvariges eller personuppgiftsbitrådets överinseende, och som får tillgång till personuppgifter, endast behandlar dessa på instruktion från den personuppgiftsansvarige, om inte unionsrätten eller medlemsstaternas nationella rätt ålägger honom eller henne att göra det.

### **GRANSKNINGEN AVSER FÖLJANDE OMRÅDEN**

Nedan framgår vilka frågor som ställts till förvaltningen och hur DSO bedömt svaren, grön markering innebär att det är bra och inte behöver vidtas någon åtgärd, gult innebär att det finns frågetecken eller brister som bör undersökas och åtgärdas, rött innebär att det finns en brist som måste åtgärdas.

	Ja, kan redogöra för samtlig verksamheter	Ja, kan redogöra för egen verksamhet	Ja, övergripande kännedom	Nej, ingen eller felaktig kunskap	Verifieringen
<b>Personuppgifter som behandlas i analoge register</b>	Aktiva före 2022 godmansskap, redovisningshandlingar				
Förekommer skyddade personuppgifter?	Ja				
Förekommer uppgifter om hälsa-sjukvård, socialtjänst eller andra uppgifter med omvänt skaderelevans?	Ja				
Förekommer uppgifter om brott?	Ja				
Förekommer andra personuppgifter som är sekretessbelagda?	Ja				
Förekommer behandling av ett större antal personer >50 och/eller ett stort antal personuppgifter?	Ja				
Förekommer uppgifter om barn?	Ja				
<b>Administration</b>					
Vet ledningen var personuppgifter förvaras?	Ja				
Finns entydigt utpekad ansvarig för förvaring och behandling av personuppgifter?	Ja				
Finns en tydlig klassning av som anger hur medarbetare ska tänka kring avvägning mellan konfidentialitet och tillgänglighet?	För skyddad personuppgift				
Finns dokumenterad rutin för åtkomst till fysiska handlingar som innehåller personuppgifter?	Inpassering				
Finns dokumenterad rutin för inventering och gallring av uppgifter/handlingar?	Informationshanteringsplan				
Har all personal som har tillgång till uppgifterna fått utbildning i förutsättningar för åtkomst och användning av uppgifterna?	Ja 5 personer				
Finns det möjlighet att följa upp åtkomst?	Loggad med inpassering				
<b>Fysisk säkerhet</b>					
Förvaras alla uppgifter på samma sätt?	Nej, olika nivå på säkerhet				
Är uppgifter förvarade i låst skåp?					
Ur uppgifterna förvarade i låst rum?	Ja				
Finns videoövervakning av förvaringen?	Nej, olika nivå på säkerhet				
Förvaras uppgifterna så att all åtkomst till dem registreras/kvitteras?	Nej, olika nivå på säkerhet				
Kan obehöriga få fysisk åtkomst till uppgifter?	Äldre handlingar i gemensamt arkiv, behöver åtgärdas				
<b>Informationssäkerhet</b>					
Finns de fysiska uppgifterna även registrerade på digitalt eller som fysisk kopia?	Inskannad handling är original				
Finns ett register över de fysiska handlingarna?	Ja, diariet				
Hur sker rättelse och komplettering av fel i de fysiska handlingarna?	Förekommer inte				
Vilket skydd finns mot obehörigt röjande, ändring, flytt eller förstöring?	Nej				
Hur kan åtkomsten till de fysiska uppgifterna begränsas?	Nej				
Finns det regler för kopiering av fysiska handlingar som innehåller personuppgifter?	Nej				
Har incidenter inträffat avseende fysiska handlingar, om så vad har de berott på?	Före GDPR handlingar har saknats i akter				
Vilka åtgärder har vidtagits för att förhindra nya incidenter?	Mkt sällsynt med incidenter				

## **DSO's bedömning**

Överförmyndarnämndens behandling av uppgifter i register präglas av att det är en liten grupp som har tillgång till och använder sig av etablerade rutiner avseende sekretess och säkerhet för handlingar och uppgifter. Då handlingar huvudsakligen hanteras som digitala original, avser förekomsten av större mängder skyddsvärda uppgifter huvudsakligen redovisningsmaterial och handlingar om godmanskap som handlades före 2022. Verksamheten använder diariet som register över handlingarna vilket möjliggör uppföljning. Då lokalerna är låsta och övervakade och det är få personer med lång erfarenhet av verksamheten som har tillgång till uppgifterna måste risken för obehörig åtkomst och röjande betraktas som låg, med undantag för de äldre handlingar som ligger i ett gemensamt arkiv. Avsaknad av skriftliga instruktioner för åtkomst till uppgifterna är utifrån förutsättningarna inte ett problem, men det skulle underlätta extern uppföljning av säkerheten.

Ledningen behöver dock kunna visa upp att uppföljning gjorts av säkerheten och att den fortsatt bedöms vara lämplig när det sker förändringar i organisation eller arbetssätt.

De åtgärder och arbetssätt som finns kring den fysiska säkerheten är efter åtgärder hur äldre handlingar förvaras väl avvägda vilket visas av få rapporterade incidenter.

## **FÖRSLAG PÅ ÅTGÄRDER**

1. Flytta de äldre handlingar som förvaras i gemensam förvaring till låst förvaring som enbart ger behörig personal åtkomst till uppgifterna.
2. Ta fram dokumenterad instruktion/rutin för hur säkerheten för personuppgifter i fysiska handlingar ska skyddas. Även om det inte upplevs som ett problem idag försvåras uppföljning utan dokumentation.