

2024 år granskningsrapport av behandling av personuppgifter i Miljö- och byggnämnden register som inte behandlas automatiskt enligt den Europeiska Dataskyddsförordningen (GDPR)

Framtagen av Regionens dataskyddsombud

Datum 20241029

Gäller

Ärendenr MBN 2024/2355

Version 1

Miljö- och byggnämnden
Region Gotland

Innehåll

Sammanfattning

Miljö- och byggnämndens behandling av personuppgifter i fysiska register uppfyller GDPR's krav på teknisk och administrativ säkerhet vid behandling av register som inte förs automatiskt, men det finns mindre avvikelser. Förvaltningens behandling av personuppgifter i register som inte förs automatiskt är av mindre omfattning, men i och med att allmänheten kan föra in uppgifter och tillståndsgivning kan innehålla skyddsvärda personuppgifter behöver förekomsten och säkerheten följas upp. Säkerheten för uppgifterna är anpassad efter skyddsvärdet då åtkomsten är begränsad till de som behöver uppgifterna.

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 medlemstaternas 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	Uppfyllelse av GDPR
Personuppgifter som behandlas i analoga register						
Förekommer skyddade personuppgifter?	Inte sedan 2018, finns alltid risk för enskilda fall					
Förekommer uppgifter om hälsa-sjukvård, socialtjänst eller andra uppgifter med omvänt skaderelevans?	Bara om registrerade själv fört in det, troligen sekretessmarkert, har funnits instruktion					
Förekommer uppgifter om brott?	Ja inom alkoholtillstånd och miljö avseende					
Förekommer andra personuppgifter som är sekretessbelagda?						
Förekommer behandling av ett större antal personer >50 och/eller ett stort antal personuppgifter?						
Förekommer uppgifter om barn?						
Administration						
Vet ledningen var personuppgifter förvaras?	Har varit objektägare för sina egna uppgifter					
Finns entydigt utpekad ansvarig för förvaring och behandling av personuppgifter?	Utsedd ansvarig, organisation klar i juni					
Finns en tydlig klassning av som anger hur medarbetare ska tänka kring avvägning mellan konfidentialitet och tillgänglighet?	Inventering gjordes 2023					
Finns dokumenterad rutin för åtkomst till fysiska handlingar som innehåller personuppgifter?	Nej					
Finns dokumenterad rutin för inventering och gallring av uppgifter/handlingar?	Informationshanteringsplanen					
Har all personal som har tillgång till uppgifterna fått utbildning i förutsättningar för åtkomst och användning av uppgifterna?	Nej, inte komplett och kommunicerad					
Finns det möjlighet att följa upp åtkomst?	Nej					
Fysisk säkerhet						
Förvaras alla uppgifter på samma sätt?	Säkerhetsnivå beroende					
Är uppgifter förvarade i låst skåp?	Bedömt					
Ur uppgifterna förvarade i låst rum?	Alkoholhandläggare					
Finns videoövervakning av förvaringen?	Nej					
Förvaras uppgifterna så att all åtkomst till dem registreras/kvitteras?	Nej					
Kan obehöriga få fysisk åtkomst till uppgifter?	Skalskydd i huset och på våningarna					
Informationssäkerhet						
Finns de fysiska uppgifterna även registrerade på digitalt eller som fysisk kopia?	Ja					
Finns ett register över de fysiska handlingarna?	Inventering 20230421					
Hur sker rättelse och komplettering av fel i de fysiska handlingarna?	Informationshanteringsplan					
Vilket skydd finns mot obehörigt röjande, ändring, flytt eller förstöring?						
Hur kan åtkomsten till de fysiska uppgifterna begränsas?						
Finns det regler för kopiering av fysiska handlingar som innehåller personuppgifter?						
Har incidenter inträffat avseende fysiska handlingar, om så vad har de berott på?	Handlingar i skrivaren, felskick					
Vilka åtgärder har vidtagits för att förhindra nya incidenter?	Follow me					

DSO's bedömning

Vid undersökningen framkom att säkerheten för behandlingen av personuppgifter i fysisk form med högre skyddsvärde, huvudsakligen rörde tillståndsgivningen där det finns etablerade rutiner avseende sekretess och säkerhet. I övriga register förekommer typiskt sätt inte några känsliga personuppgifter såvida de inte förts in av någon som är part i handläggningen, vilket gör att uppgifterna inte är sökbart. De uppgifter som hanteras utanför de digitala systemen är även på väg att digitaliseras, vilket minskar riskerna, men samtidigt kan utvecklas till en tillgänglighetsrisk vid störningar. Styrningen av säkerheten för de fysiska registren är aningen vag, men då det huvudsakligen inte rör känsliga uppgifter är det i praktiken inte något större problem. Om det av något skäl blir aktuellt att börja behandla fler uppgifter i fysiska register behöver dock struktur och styrning ses över.

Det finns ett värde i att förvaltningen själva tar ställning till om man anser att nuvarande anvisningar och instruktioner till medarbetarna är tillräckliga, eller om det finns områden där det bör kompletteras. Ledningen behöver dock kunna visa upp att uppföljning gjorts av säkerheten och att den bedöms vara lämplig när det sker förändringar i organisation eller arbetssätt.

De åtgärder och arbetssätt som finns kring den fysiska säkerheten är i praktiken väl avvägda vilket styrks av att de incidenter som berör fysiska handlingar är kopplade till felutskick och försvunna utskrifter.

FÖRSLAG PÅ ÅTGÄRDER

1. Ta fram dokumenterad instruktion/rutin för hur personuppgifter i fysiska handlingar ska skyddas. Även om det inte upplevs som ett problem idag försvåras uppföljning utan dokumentation.
2. Inför follow me utskrifter