NORRTÄLJE KOMMUN

xPersonuppgiftsansvarig
Socialkontoret
Rapporterat av Nicklas Söderblom Gräns, Enhetschef

Egenkontrollplan för GDPR

Datum: 2024-09-26

Egenkontrollplan för GDPR

Detta dokument sammanfattar de krav som ställs i dataskyddsförordningen (GDPR) vid behandling av personuppgifter. Personuppgifter är varje typ av information som kan kopplas till en individ i livet. Nedan listas ett antal krav (kontrollpunkter), fördelat på nio områden, som i stort motsvarar samtliga krav enligt GDPR.

Dokumentet är både ett underlag för dataskyddsombudet (DSO) i sitt uppdrag att granska efterlevnaden av dataskyddsförordningen och ett sätt för varje verksamhet att kontrollera att dataskyddsförordningens krav följs.

I slutet av dokumentet finns mer information om respektive kontrollpunkter.

Kontrollpunkt (krav enligt GDPR)	**Uppfylls (ja/delvis/nej) Poäng (0-5)**	**Kommentar (motivera bedömningen)**	**Poängsättning efter dialogmöte (0-5)**
1. REGISTRERA PERSONUPPGIFTSBEHANDLINGAR			
Verksamhetens behandlingsregister är komplett[1]	**3**	**Inte fullständigt antal registerförteckningar**	**2,0 behöver komplettera registerförteckningen med bättre beskrivningar och de som saknas**
Informationen i behandlingsregister är aktuell	**3**	**Inte fullständigt uppdaterade registerförteckningar**	

[1] Med komplett menas att samtliga processer där personuppgifter hanteras är dokumenterade i behandlingsregistret (Drafit records). En utomstående ska kunna förstå vilka personuppgifter verksamheten hanterar och varför.

Kontrollpunkt (krav enligt GDPR)	Uppfylls (ja/delvis/nej) Poäng (0-5)	Kommentar (motivera bedömningen)	Poängsättning efter dialogmöte (0-5)
2. GRUNDLÄGGANDE PRINCIPER			
Verksamheten har kännedom om de grundläggande principer och dessa beaktas i verksamhetens arbete som rör personuppgifter	**3**	**Kan bli bättre men förhållandevis god kännedom**	**4,5 egen utbildning gjord som specificerar vad som gäller Soc. Tanke finns att skapa årshjul när utbildningarna ska göras**
Verksamhetens medarbetare har genomfört grundläggande utbildning i GDPR	**4**	Socialkontoret har sedan ikraftträdandet av GDPR genomfört utbildningar för samtliga nyanställda, samt en gemensam utbildning för hela förvaltningen per år. Därutöver har vi nu börjat med en GDPR utbildning med inriktning på socialtjänsten i Mitt lärande. Den har 44% av socialkontorets medarbetare genomfört sedan 30 augusti 2024. Samtliga medarbetare ska ha genomfört utbildningen sista oktober 2024.	

Kontrollpunkt (krav enligt GDPR)	Uppfylls (ja/delvis/nej) Poäng (0-5)	Kommentar (motivera bedömningen)	Poängsättning efter dialogmöte (0-5)
Verksamheten använder samtycke som rättslig grund enbart i situationer då kriteriet för frivillighet uppfylls.		**Vi använder aldrig samtycke som rättslig grund.**	
3. RAPPORTERA PERSONUPPGIFTSINCIDENTER			
Verksamhetens medarbetare är informerade om definitionen och processen för personuppgiftsincidenter (på en introduktion, minst årligen på APT eller liknande)	**5**	**Välfungerande process för anmälan och hantering av personuppgiftsincidenter. Gemensam utbildning en gång per år för samtliga medarbetare och löpande på APT efter behov per enhet.**	**4,0 pga mörkertal, blir en höjning av anmälningarna vid utbildning**
Verksamhetens medarbetare rapporterar in personuppgiftsincidenter i relevant omfattning	**4**	**Kan alltid bli bättre.**	
Samtliga inrapporterade incidenter under året är färdigdokumenterade och avslutade i Platina[2]	**5**	**Vissa är givetvis fortsatt pågående, särskilt de som inväntar svar från IMY.**	

[2] Om incidenten är färdigbehandlad. Ärenden som anmälts till IMY men där IMY inte ännu återkopplat ska hållas öppna tills återkoppling fås.

Kontrollpunkt (krav enligt GDPR)	Uppfylls (ja/delvis/nej) Poäng (0-5)	Kommentar (motivera bedömningen)	Poängsättning efter dialogmöte (0-5)
Incidenterna har följts upp och föreslagna åtgärder har vidtagits.	**5**		
4. KONSEKVENSBEDÖMNINGAR (DPIA)			
Verksamheten har bedömt och dokumenterat om en personuppgiftsbehandling kräver en konsekvensbedömning (DPIA)	**4**	**Ja, när behov uppstår. Har dock inte landat i behov av någon DPIA.**	**2,0 kommer göras vid nya behandlingar. De som gjorts har blivit gamla och bör följas upp**
Verksamheten har rutiner för att säkerställa att konsekvensbedömningar görs för framtida personuppgiftsbehandlingar, där så krävs			
Planerade konsekvensbedömningar har genomförts[3]			
Åtgärder i genomförda konsekvensbedömningar finns intagna i en handlingsplan, förvaltningsplan eller liknande			
5. PERSONUPPGIFTSBITRÄDEN			

[3] Konsekvensbedömningar ska i regel göras innan en personuppgiftsbehandling påbörjas, ex. innan ett nytt system köps in eller ett nytt arbetssätt introduceras.

Kontrollpunkt (krav enligt GDPR)	**Uppfylls (ja/delvis/nej) Poäng (0-5)**	**Kommentar (motivera bedömningen)**	**Poängsättning efter dialogmöte (0-5)**
Verksamheten har kartlagt sina samtliga externa parter/leverantörer[4] och bedömt ifall dessa är personuppgiftsbiträde/gemensamt personuppgiftsansvarig	**2**	**Vi har inte ens reglerat förhållande inom kommunen. Vi är betydligt bättre med externa aktörer från privata sektorn.**	**3,0. Bättre att följa upp med leverantören, reglemente saknas.**
Verksamheten har tecknat personuppgiftsbiträdesavtal (PUB-avtal) med sina biträden eller reglerat dessa i ett reglemente (gäller mellan nämnder)	**2**	**Vi har inte ens reglerat förhållande inom kommunen. Vi är betydligt bättre med externa aktörer från privata sektorn.**	
Verksamheten har kontrollerat om personuppgifter överförs till tredje land (ett land utanför EU/ESS)[5]. Om uppgifter överförs till tredjeland har lagligheten kontrollerats.	**4**	**Är med som en bedömning inför anlitandet av en leverantör.**	
Verksamheten har följt upp personuppgiftsbiträdesavtalen[6]	**1**	**Vi behöver bli MYCKET bättre på uppföljningen. Har enbart gjort vid uppenbara behov.**	

4 Dvs. kontrollerat vilka externa parter behandlar verksamhetens personuppgifter - genom lagring, åtkomst, överföring eller liknande.
5 Tredjelandsöverföring sker när personuppgifter behandlas i ett land utanför EU/EES. Tredjelandsöverföring omfattar även underbiträden till personuppgiftsbiträden (PUB). Det betyder att verksamheten behöver kontrollera vilka underbiträden ett personuppgiftsbiträde anlitar. Tredjelandsöverföring är enbart tillåten under särskilda förutsättningar och lagligheten måste därför kontrolleras.
6 Behöver göras regelbundet, ju känsligare personuppgifter biträdet hanterar desto viktigare är att uppföljning görs återkommande. Uppföljningen kan med fördel genomföras inom portföljstyrningen.

Kontrollpunkt (krav enligt GDPR)	Uppfylls (ja/delvis/nej) Poäng (0-5)	Kommentar (motivera bedömningen)	Poängsättning efter dialogmöte (0-5)
6. ARKIVERING OCH GALLRING			
Verksamhetens informationshanteringsplan/ hanteringsanvisningar är upprättad, komplett och aktuell	**4**	**Ny går upp i nästa nämnd.**	**4,5 Hanteringsanvisningar uppdateras regelbundet**
Arkivering och gallring genomförs enligt informationshanteringsplanen/ hanteringsanvisningar	**4**	**Haft vissa problem med E-tjänster och verksamhetssystem, fungerar generellt bra.**	
7. REGISTRERADES RÄTTIGHETER			
Verksamheten har rutiner för utlämnade av registerutdrag (rätten till tillgång)[7]	**5**		**3,5 behöver kompletteras med specifika behandlingar som gäller Soc till externa webben**
Verksamheten har informerat enskilda om hur personuppgifter hanteras (rätt till information)	**3**	**Ja, men skulle behöva uppdatera informationen – samt tydliggöra på hemsidan.**	

[7] Rutinen ska säkerställa att information i samtliga lagringsytor/system som verksamheten ansvarar för söks igenom och att den information som lämnas motsvarar kraven i GDPR.

Kontrollpunkt (krav enligt GDPR)	Uppfylls (ja/delvis/nej) Poäng (0-5)	Kommentar (motivera bedömningen)	Poängsättning efter dialogmöte (0-5)
Verksamheten har en rutin/process för att hantera övriga rättigheter, dvs. begäran om radering, rättelse, invändning och begränsning (samt dataportabilitet, om tillämplig)	**4**	**Inte lika aktuell som utlämnande då detta inte händer lika ofta.**	
Om automatiskt beslutsfattande används, har verksamheten kontrollerat att det är förenligt med artikel 22 GDPR			
8. KÄNSLIGA OCH EXTRA SKYDDSVÄRDA PERSONUPPGIFTER			
Om verksamheten hanterar känsliga personuppgifter, har det säkerställts att ett undantag enligt artikel 9 GDPR finns.	**5**		**4,0 behöver dokumenterat den rättsliga grunden men arbetar med frågor**
Verksamheten har rutiner för hur och var känsliga och extra skyddsvärda personuppgifter får hanteras. Rutinerna har kommunicerats till medarbetare (på introduktion, årligen på APT eller liknande)	**5**	**Hanteringsanvisningar**	
9. INFORMATIONSSÄKERHET			

Kontrollpunkt (krav enligt GDPR)	**Uppfylls (ja/delvis/nej) Poäng (0-5)**	**Kommentar (motivera bedömningen)**	**Poängsättning efter dialogmöte (0-5)**
Verksamheten har informationsklassat sina informationstillgångar	1	Pågående arbete.	2,5 behöver klassa vidare och få ett systematiskt arbetssätt
Verksamhetens system har framtagen handlingsplan i verktyget KLASSA[8]	1	Pågående arbete.	
Åtgärder från handlingsplanen i KLASSA finns intagen i systemets förvaltningsplan[9]	1	Pågående arbete.	
Verksamheten har behörighetsstyrt tillgång till verksamhetens personuppgifter enligt principen lägsta behörighet[10]	4	Inte fullt ut, saknar optimal styrning i vissa system. Generellt och för de viktigaste – ja.	
Verksamhetens riskanalyser inkluderar även informationssäkerhet (RSA)	3	Beror på typ av riskanalys, är inte med i samtliga.	
Verksamheten har med informationsrisker i sin kontinuitetsplan	4	Ja, utifrån de prioriterade åtaganden vi identifierat i verksamheten.	

[8] Leds av portföljansvarig.
[9] Leds av portföljansvarig.
[10] Dvs. att åtkomst till information enbart ges till de som behöver informationen för sitt arbete.

Sammanfattning av krav enligt dataskyddsförordningen GDPR

1. Registrera personuppgiftsbehandlingar

En förutsättning för att överhuvudtaget kunna efterleva dataskyddsförordningens regler är att veta vilka personuppgifter som behandlas och varför. Varje personuppgiftsansvarig ska enligt artikel 30 ha en förteckning (behandlingsregistret) över sina personuppgiftsbehandlingar där bland annat syfte, typer av personuppgifter och lagringstid framgår.

I Norrtälje registreras personuppgiftsbehandlingar i systemet Draftit records. Detta görs oftast av en dataskyddssamordnare eller annan utsedd person i verksamheten.

Relevant länk för mer information:
Föra register över personuppgiftsbehandlingar | IMY

2. Dataskyddsprinciperna

Grundläggande principer för behandling av personuppgifter anges i artikel 5 i dataskyddsförordningen. Principerna fungerar som vägledning för hur personuppgifter får hanteras och genomsyrar även övriga krav på dataskydd. Därför är det viktigt att känna till principerna och beakta dessa i frågor som rör personuppgifter. Det handlar bland annat om att ha en rättslig grund, enbart behandla så många personuppgifter som behövs för ett visst syfte, inte spara längre än de behövs och ha tillräcklig säkerhet.

De grundläggande principerna:

- Laglighet, korrekthet och öppenhet
- Ändamålsbegränsning
- Uppgiftsminimering
- Riktighet
- Lagringsminimering
- Integritet och konfidentialitet
- Ansvarsskyldighet

Relevant länk för mer information:
Grundläggande principer enligt GDPR | IMY

Genomförd grundutbildning i GDPR i mitt lärande (LMS) eller motsvarande för bolagen.
Mitt lärande

3. Rapportera personuppgiftsincidenter

Varje verksamhet ska ha processer för att upptäcka, utreda, åtgärda och anmäla personuppgiftsincidenter. Vissa personuppgiftsincidenter ska även anmälas till Integritetsskyddsmyndigheten (IMY). Det innebär att medarbetare ska kunna identifiera när en personuppgiftsincident har hänt, veta hur den ska rapporteras och att det finns processer för att ta hand om en bekräftad incident. Det är även av vikt att incidenten leder till uppdaterade rutiner och arbetssätt för att förhindra nya incidenter.

Relevant länk för mer information:
Personuppgiftsincidenter | IMY

4. Konsekvensbedömning (DPIA)

Om det finns en hög risk för enskildas fri- och rättigheter när personuppgifter behandlas, ska en konsekvensbedömning (DPIA – Data Protection Impact Assessment) göras. Konsekvensbedömningens syfte är både att säkerställa att enskildas fri- och rättigheter respekteras och är även ett sätt att visa att dataskyddsförodningen följs.

Relevant länk för mer information:
Konsekvensbedömningar och förhandssamråd | IMY

5. Personuppgiftsbiträdesavtal (PUB-avtal) /Reglemente

Personuppgiftsbiträdesavtal ska tecknas om en personuppgiftsansvarig anlitar en extern part/leverantör som behandlar personuppgifter åt den personuppgiftsansvariga. Reglemente ska upprättas mellan nämnder i stället för personuppgiftsbiträdesavtal. Den externa parten/leverantören är då biträde och avtalet ska reglera att personuppgifter behandlas och skyddas efter instruktioner från den personuppgiftsansvarige.
Om två parter gemensamt bestämmer syftet rör det sig om ett gemensamt personuppgiftsansvar och då ska ett datadelningsavtal upprättas.

Relevant länk för mer information:
Vägledande kommentarer, PUB-avtal | SKR

6. Lagringsminimering, arkivering och gallring

Lagringsminimering är en av dataskyddsprinciperna som anger att personuppgifter endast får behandlas så länge de behövs för ändamålet. Lagringsminimering innebär att det ska vara ordning och reda bland verksamhetens information, att information arkiveras och gallras enligt informationshanteringsplanen/hanteringsanvisningarna.

Relevant länk för mer information:
Dokument och ärendehantering

7. Registrerades rättigheter

Registrerade har ett antal rättigheter avseende sina personuppgifter:

- Rätt att kontakta en personuppgiftsansvarig för att få besked om ens personuppgifter behandlas och i så fall få tillgång till dessa (Rätt till tillgång – även kallat ”registerutdrag”)
- Rätt att få information om vilka personuppgifter hanteras och hur de används (rätten till information)
- Under vissa förutsättningar få sina uppgifter raderade eller rättade (rätten till radering och rättelse)
- Rätt att invända, dvs. motsätta sig, mot en personuppgiftsbehandling och även begära begränsning av dessa (Rätten att göra invändningar och begära begränsning)
- Rätt att inte bli föremål för automatiskt beslutsfattande[11]
- Rätt att få ut sina personuppgifter på ett strukturerat sätt för att använda de hos någon annan (rätt till dataportabilitet – gäller enbart i få specifika fall inom offentlig förvaltning)

Verksamheter hanterar generellt personuppgifter i stor omfattning vilket kräver att det finns utarbetade processer på plats om hur en enskild kan utöva sina rättigheter, särskilt vad gäller rätten till tillgång (registerutdrag).

Relevant länk för mer information:
Rätt till information om hur dina personuppgifter hanteras | IMY

[11] Beslut som fattas utan att en fysisk person är inblandad.

8. Känsliga och extra skyddsvärda personuppgifter

Det finns ett generellt förbud mot att använda känsliga personuppgifter[12] i dataskyddsförordningen. Behandling av känsliga personuppgifter är enbart tillåtet om något av undantagen är tillämpligt. Det finns personuppgifter som kallas extra skyddsvärda[13] dessa kräver inte ett undantag för att det ska vara tillåtet att behandla dem. Behandling av känsliga och extra skyddsvärda personuppgifter kräver att de skyddas med höga säkerhetsåtgärder (tekniska och organisatoriska).

Relevanta länkar:
Anvisning informationsklassificering
Anvisning informationshantering
Informationssäkerhet på intranätet

9. Informationssäkerhet

Integritet och konfidentialitet är en dataskyddsprincip som handlar om att säkerställa att inga personuppgifter röjs för obehöriga (konfidentialitet), är tillgängliga när de behövs (tillgänglighet) och är korrekta (riktighet). Detta säkerställs genom ett aktivt informationssäkerhetsarbete.

Relevanta länkar:
Informationssäkerhet på intranätet

---

[12] Beskrivning av känsliga personuppgifter, se: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter
[13] Beskrivning av extra skyddsvärda personuppgifter, se: https://www.imy.se/verksamhet/dataskydd/det-har-galler-enligt-gdpr/introduktion-till-gdpr/personuppgifter/kansliga-personuppgifter