NACKA KOMMUN

Kontrollpunkter
Datakyddsombudets
årsrapport 2021

1. Registrera personuppgiftsbehandlingar

Kontrollpunkt
Enhetens/verksamhetens registerförteckning är komplett[1]
Informationen i registerförteckningen är aktuell
Registerförteckningen speglar den publika presentationen av nämndens personuppgiftsbehandlingar på nacka.se[2]

2. Grundläggande principer

Kontrollpunkt
Enheten/verksamheten har kontrollerat att varje personuppgiftsbehandling följer de grundläggande principerna[3]
Enheten/verksamheten använder samtycke som rättslig grund enbart i situationer då kriteriet för frivillighet uppfylls

3. Rapportera personuppgiftsincidenter

Kontrollpunkt
Medarbetare är informerade om definitionen och processen för personuppgiftsincidenter (på en introduktion, minst årligen på APT eller liknande)
Samtliga inrapporterade incidenter under året är färdigdokumenterade och avslutade i Platina[4]
Incidenterna har följts upp och föreslagna åtgärder har vidtagits

[1] Med komplett menas att samtliga processer där personuppgifter hanteras är dokumenterade i registerförteckningen. En utomstående ska kunna förstå vilka personuppgifter enheten hanterar och varför.
[2] https://www.nacka.se/om-webbplatsen/behandling-av-personuppgifter/ under rubrik ”Beskrivning av de personuppgiftsbehandlingar vi utför”
[3] Se checklista på följande sida:
https://nacka.sharepoint.com/sites/DataskyddsforumNacka/SitePages/Grundl%C3%A4ggande-principer-(Dataskyddsprinciperna).aspx
[4] Om incidenten är färdigbehandlad. Ärenden som anmälts till IMY men där IMY inte ännu återkopplat ska hållas öppna tills återkoppling fås.

4. Konsekvensbedömning (DPIA)

Kontrollpunkt
Enheten/verksamheten har kontrollerat om någon av personuppgiftsbehandlingarna kräver en konsekvensbedömning (DPIA)[5]
Enheter/verksamheten har rutiner för att säkerställa att konsekvensbedömningar görs för framtida personuppgiftsbehandlingar, där så krävs[6]
Planerade konsekvensbedömningar har genomförts[7]
Åtgärder i genomförda konsekvensbedömningar finns intagna i en handlingsplan, förvaltningsplan eller liknande

5. Personuppgiftsbiträdesavtal (PUB-avtal)

Kontrollpunkt
Enheten/verksamheten har kartlagt sina samtliga externa parter/leverantörer[8] och bedömt ifall parten/leverantören är personuppgiftsbiträde/gemensamt personuppgiftsansvarig
Enheten/verksamheten har tecknat personuppgiftsbiträdesavtal (PUB-avtal), där det behövs
Enheten/verksamheten har kontrollerat om personuppgifter överförs till tredje land (ett land utanför EU/ESS)[9]. Om uppgifter överförs till tredjeland har lagligheten kontrollerats.

5 Kriterier som utgör ”hög risk” och därmed leder till att en konsekvensbedömning krävs finns i mallen för konsekvensbedömningar (DPIA), se https://www.nacka.se/globalassets/medarbetare/juridik/dokument/mallar-gdpr/konsekvensbedomning-dpia-mall.docx

6 Exempelvis genom att säkerställa att varje digitaliseringsärende går igenom beredningsgruppen, läs mer: https://www.nacka.se/medarbetare/digitalisering/om-digitalisering-i-nacka/vad-gor-beredningsgruppen

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

8 Dvs. kontrollerat vilka externa parter behandlar nämndens personuppgifter - genom lagring, åtkomst, överföring eller liknande.

9 Kontakta dataskyddsombudet om ni överför personuppgifter till tredje land. Tredjelandsöverföring sker när uppgifter lagras, skickas eller ges åtkomst till från ett land utanför EU/EES. Vanligtvis sker tredjelandsöverföring genom att ett personuppgiftsbiträde anlitar ett underbiträde utanför EU/ESS. Det betyder att enheten/verksamheten måste kontrollera vilka underbiträden ett biträde anlitar. Tredjelandsöverföring är enbart tillåten under särskilda förutsättningar och lagligheten måste därför kontrolleras.

Enheten har följt upp personuppgiftsbiträdesavtalen[10]

6. Lagringsminimering, arkivering och gallring

Kontrollpunkt
Enhetens informationshanteringsplan är upprättad, komplett och aktuell
Arkivering och gallring genomförs enligt informationshanteringsplanen
Information som inte längre behövs och faller utanför informationshanteringsplanen[11] rensas regelbundet

7. Registrerades rättigheter

Kontrollpunkt
Enheten/verksamheten har rutiner för utlämnade av registerutdrag (rätten till tillgång)[12]
Enheten/verksamheten har informerat enskilda om hur personuppgifter hanteras (rätt till information)
Enheter har en rutin/process för att hantera övriga rättigheter, dvs. begäran om radering, rättelse, invändning och begränsning (samt dataportabilitet, om tillämplig)
Om enheten/verksamheten använder sig av automatiskt beslutsfattande, finns möjlighet för en registrerad att inte blir föremål för detta

8. Känsliga och extra skyddsvärda personuppgifter

Kontrollpunkt
Om enheten/verksamheten hanterar känsliga personuppgifter, har det säkerställts att ett undantag enligt artikel 9 finns.
Enheten/verksamheter har rutiner för hur och var känsliga och extra skyddsvärda personuppgifter får hanteras

[10] Behöver ej göras årligen, men ju känsligare personuppgifter biträdet hanterar desto viktigare är att uppföljning görs återkommande. Uppföljningen kan med fördel genomföras inom system/objektförvaltningen.
[11] Kopior, utkast, osv. som ej räknas som allmänna handlingar och som inte längre behövs.
[12] Inom kommunens nämnder samordnas registerutdraget centralt av Kundserviceenheten, men respektive enhet/verksamhet är ansvarig för att hantera en begäran inom sitt ansvarsområde. Rutinen ska säkerställa att information i samtliga lagringsytor/system som enheten/verksamheten ansvarar för söks igenom och att den information som lämnas motsvarar kraven i GDPR.

Rutinerna har kommunicerats till medarbetare (på introduktion, årligen på APT eller liknande)
Personuppgiftsbiträden som behandlar känsliga personuppgifter för nämndens räkning har identifierats och biträdets hantering följs upp återkommande[13]

9. Informationssäkerhet

Kontrollpunkt
Informationen i enhetens/verksamhetens system har informationsklassats
Enhetens/verksamhetens arbete med riskanalyser inkluderar även informationssäkerhet
Det befintliga skyddet i enhetens/verksamhetens system har bedömts i verktyget KLASSA[14]
Handlingsplanen i KLASSA finns intagen i systemets förvaltningsplan[15]
Enheten/verksamheten har behörighetsstyrt tillgång till enhetens/verksamhetens personuppgifter enligt principen lägsta behörighet[16]

13 Görs med fördel inom system/objektförvaltningen.
14 Görs av förvaltningsledare/objektsledare.
15 Görs av förvaltningsledare/objektsledare
16 Dvs. att åtkomst till information enbart ges till de som behöver informationen för sitt arbete.