

## 1. Registrera personuppgiftsbehandlingar

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

## 2. Grundläggande principer

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

## 3. Rapportera personuppgiftsincidenter

<b>Kontrollpunkt</b>
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 <sup>4</sup>
Incidenterna har följts upp och föreslagna åtgärder har vidtagits

<sup>1</sup> Med komplett menas att samtliga processer där personuppgifter hanteras är dokumenterade i registerförteckningen. En utomstående ska kunna förstå vilka personuppgifter enheten hanterar och varför.

<sup>2</sup> <https://www.nacka.se/om-webbplatsen/behandling-av-personuppgifter/> under rubrik ”Beskrivning av de personuppgiftsbehandlingar vi utför”

<sup>3</sup> Se checklista på följande sida:

[https://nacka.sharepoint.com/sites/DataskyddforumNacka/SitePages/Grundl%C3%A4ggande-principer-\(Dataskyddsprinciperna\).aspx](https://nacka.sharepoint.com/sites/DataskyddforumNacka/SitePages/Grundl%C3%A4ggande-principer-(Dataskyddsprinciperna).aspx)

<sup>4</sup> 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) <sup>5</sup>
Enheter/verksamheten har rutiner för att säkerställa att konsekvensbedömningar görs för framtida personuppgiftsbehandlingar, där så krävs <sup>6</sup>
Planerade konsekvensbedömningar har genomförts <sup>7</sup>
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 <sup>8</sup> 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) <sup>9</sup> . Om uppgifter överförs till tredjeland har lagligheten kontrollerats.

<sup>5</sup> 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>

<sup>6</sup> 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>

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

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

<sup>9</sup> Kontakta dataskyddsbudet 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<sup>10</sup>

## 6. Lagringsminimering, arkivering och gallring

<b>Kontrollpunkt</b>
Enhetens informationshanteringsplan är upprättad, komplett och aktuell
Arkivering och gallring genomförs enligt informationshanteringsplanen
Information som inte längre behövs och faller utanför informationshanteringsplanen <sup>11</sup> rensas regelbundet

## 7. Registrerades rättigheter

<b>Kontrollpunkt</b>
Enheten/verksamheten har rutiner för utlämnade av registerutdrag (rätten till tillgång) <sup>12</sup>
Enheten/verksamheten har informerat enskilda om hur personuppgifter hanteras (rätt till information)
Enheten 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

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

<sup>10</sup> 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.

<sup>11</sup> Kopior, utkast, osv. som ej räknas som allmänna handlingar och som inte längre behövs.

<sup>12</sup> Inom kommunens nämnder samordnas registerutdraget centralt av Kundenserviceenheten, 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 bitrådets hantering följs upp återkommande<sup>13</sup>

## 9. Informations säkerhet

### Kontrollpunkt

Informationen i enhetens/verksamhetens system har informationsklassats

Enhetens/verksamhetens arbete med riskanalyser inkluderar även informations säkerhet

Det befintliga skyddet i enhetens/verksamhetens system har bedömts i verktyget KLASSA<sup>14</sup>

Handlingsplanen i KLASSA finns intagen i systemets förvaltningsplan<sup>15</sup>

Enheten/verksamheten har behörighetsstyrt tillgång till enhetens/verksamhetens personuppgifter enligt principen lägsta behörighet<sup>16</sup>

<sup>13</sup> Görs med fördel inom system/objektförvaltningen.

<sup>14</sup> Görs av förvaltningsledare/objektsledare.

<sup>15</sup> Görs av förvaltningsledare/objektsledare

<sup>16</sup> Dvs. att åtkomst till information enbart ges till de som behöver informationen för sitt arbete.