

# Kontrollplan för granskning av verksamheternas dataskyddsar- bete 2023

# Innehåll

<b>Kontrollplan för granskning av verksamheternas dataskyddsarbete 2023</b>	<b>1</b>
<b>1. Bakgrund</b>	<b>3</b>
1.1 Dataskyddsförordningen	3
<b>2. Kontrollplan för dataskyddsarbetet</b>	<b>3</b>
2.1 Syfte och mål	3
2.3 Upplägg	4
2.4 Tidplan för kontroller 2023	4
<b>3. Kontrollpunkter</b>	<b>4</b>
3.1 Fasta kontrollpunkter	4
3.2 Fördjupad kontroll 2023	6
<b>4. Uppföljning</b>	<b>8</b>
4.1 Uppföljning av lämnade rekommendationer	8
<b>5. Rapportering</b>	<b>8</b>
5.1 Delrapportering	8
5.2 Årsrapport	8
5.3 Särskilt yttrande till högsta ledning	8
5.4 Beslutanderätten i dataskyddsfrågor	9
<b>6. Kontakt</b>	<b>9</b>

# 1. Bakgrund

## 1.1 Dataskyddsförordningen

Dataskyddsförordningen (DSF) trädde i kraft i maj 2018 och syftar till att skydda fysiska personers grundläggande fri- och rättigheter samt att garantera ett likvärdigt skydd samt att säkerställa det fria flödet av personuppgifter inom unionen. Dataskyddsförordningen ställer höga krav på Regionens behandling av personuppgifter. Utöver att insamlingen av personuppgifterna ska vara tillåten, måste den personuppgiftsansvarige dessutom hantera dessa uppgifter på ett korrekt sätt, med respekt för den enskildes integritet och med beaktande av lämpliga säkerhetsåtgärder. Efterlevnaden av lagstiftningen övervakas av Integritetsskyddsmyndigheten och överträdelser kan leda till bland annat sanktionsavgifter eller skadestånd.

### 1.1.1 Personuppgiftsansvarig

Varje nämnd och styrelse i Regionen räknas som en egen myndighet, i juridisk mening, varje enskild nämnd eller styrelse är därför ansvarig för att de personuppgiftsbehandlingar som verksamheten hanterar utförs i enlighet med gällande regelverk. För att följa dataskyddsarbetet och hålla nämnden/styrelsen informerad bör enligt dataskyddsförordningen ett dataskyddsombud utses för att bistå den ansvarige med att övervaka efterlevnaden av förordningen.

### 1.1.2 Dataskyddsombud

Dataskyddsombudet ska ge råd och information till den personuppgiftsansvarige samt övervaka efterlevnaden av dataskyddsförordningen och annan relevant dataskyddslagstiftning. Det innebär bland annat att kontrollera hur den personuppgiftsansvarige behandlar personuppgifter, att bestämmelser och interna styrdokument följs samt att ge råd och stöd vid konsekvensbedömningar. Dataskyddsombudet ska enligt dataskyddsförordningen utföra sitt arbete på ett oberoende sätt gentemot den som är personuppgiftsansvarig och får inte instrueras av denne hur arbetet ska utföras. Dataskyddsombudet är inte ansvarig för att lagstiftningen efterlevs i verksamheten.

# 2. Kontrollplan för dataskyddsarbetet

## 2.1 Syfte och mål

Dataskyddsombudets uppgift att övervaka den personuppgiftsansvariges efterlevnad av förordningen regleras i artikel 39. En del av denna övervakning innebär att dataskyddsombudet genomför kontroller av dataskyddsarbetet inom Regionen. Dessa kontroller specificeras genom denna kontrollplan som syftar till att informera personuppgiftsansvariga om tidplan och särskilda fokusområden för kontrollarbetet år 2023. Målet med att på förhand fastställa en kontrollplan är att det ska bidra till att sätta fokus på verksamhetens dataskyddsarbete och därmed också driva dataskyddsarbetet framåt i Regionen.

Dataskyddsombudet ska arbeta utifrån en riskbaserad metod. Primära fokusområden och prioriteringar utgår från eventuella områden som i högre grad påverkar de registrerades rättigheter men också Regionens förmåga att bedriva ett säkert dataskyddsarbete.

## 2.3 Upplägg

Kontrollarbetet består av tre delar som tillsammans syftar till att ge såväl data-skyddsombud som personuppgiftsansvariga en överblick över verksamhetens data-skyddsarbete och dess följsamhet gentemot förordningen.

- a) En del av granskningen består av fasta kontrollpunkter där varje punkt bedöms årligen. Bedömningen görs genom löpande kontroller, genom deltagande i verksamhetens arbete och i förekommande fall utifrån given information.
- b) Den andra delen av granskningen är en fördjupad kontroll av utvalda verksamhetsspecifika kontrollpunkter.
- c) Den tredje delen är en uppföljning och bedömning av hur verksamheten hantarerat tidigare lämnade rekommendationer.

Kontrollarbetets olika delar sammanställs och presenteras i årsrapporten för nämnd/styrelse. Identifierade aktiviteter kan komma att behöva justeras utifrån händelser som inträffar i verksamheterna eller i omvärlden.

## 2.4 Tidplan för kontroller 2023

Månad	Aktivitet	Övriga aktiviteter
Januari	Kontrollplan för året lämnas till nämnder och styrelse.	
Februari-Maj	Fördjupad kontroll av utvalda verksamhetsspecifika kontrollpunkter genomförs	Utbildningstillfällen
September- November	Uppföljning av tidigare lämnade rekommendationer  Kontroll av fasta kontrollpunkter	Utbildningstillfällen
December	Årsrapport lämnas till nämnder/styrelse	

## 3. Kontrollpunkter

### 3.1 Fasta kontrollpunkter

De fasta kontrollpunkternas utgångspunkt är Dataskyddsförordningens grundläggande principer. Verksamhetens följsamhet mot förordningen beror till stor del på hur väl dessa principer har integrerats i verksamhetens ordinarie processer.

Med principerna som utgångspunkt har åtta kontrollpunkter definierats, av både organisatorisk och teknisk karaktär, vilka är gemensamma för alla

verksamheter inom Region Västerbotten. Syftet med arbetssättet är att skapa ett arbetssätt som hanterar punkterna så att kontrollerna över tid kommer att kräva mindre och mindre arbete.

#### Kontrollpunkter

1. Styrdokument för dataskyddsarbetet
2. Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingen
3. Personuppgiftsincidenter
4. Personuppgiftsbiträdesavtal
5. Registerförteckning
6. Konsekvensbedömning/samråd
7. Hantering av registrerade rättigheter
8. Kunskapsnivån i verksamheten

### **3.1.1 Beskrivning av fasta kontrollpunkter**

#### ***Kontrollpunkt 1: Styrdokument för dataskyddsarbetet***

Kontrollpunkten avser verksamhetens organisatoriska förutsättningar för att kunna bedriva ett kontinuerligt dataskyddsarbete, och omfattar bland annat verksamhetens dataskyddsorganisation, definierade ansvarsområden och rapporteringsvägar för involverade funktioner samt tillhandahållna resurser för arbetet.

#### ***Kontrollpunkt 2: Tekniska och organisatoriska åtgärder för personuppgiftsbehandlingen***

Kontrollpunkten avser regionens förmåga att säkerställa att tekniska och organisatoriska åtgärder vidtas till skydd för personuppgifterna. Regionen ansvarar för att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas. Vilka säkerhetsåtgärder som är lämpliga beror bland annat på hur känslig behandlingen är, vilka risker som finns för de anställda och vilka tekniska lösningar som är tillgängliga. Exempel på tekniska säkerhetsåtgärder är inloggning, behörighetsspärrar, brandväggar, kryptering, pseudonymisering, säkerhetskopiering och antiviruskydd. Organisatoriska säkerhetsåtgärder handlar om det administrativa säkerhetsarbetet som till exempel tilldelning av åtkomsträttigheter, interna rutiner, instruktioner och riktlinjer.

#### ***Kontrollpunkt 3: Personuppgiftsincidenter***

Kontrollpunkten avser verksamhetens förutsättningar att identifiera och hantera personuppgiftsincidenter. För att uppfylla ansvarsskyldigheten bör verksamhetens rutin för hanteringen vara dokumenterad. I de fall verksamheten är både personuppgiftsansvarig och personuppgiftsbiträde bör rutinen omfatta båda scenarier. I kontrollpunkten ingår även översyn av verksamhetens rutin för att bedöma incidenten, hantering av eventuell anmälan till tillsynsmyndigheten samt hur rutinerna tillgängliggörs och kommuniceras inom verksamheten. Även efterlevnad av verksamhetens dokumentationsskyldighet, att alla inträffade personuppgiftsincidenter registreras, innefattas.

#### ***Kontrollpunkt 4: Personuppgiftsbiträdesavtal***

Kontrollpunkten avser verksamhetens dokumentation av biträdesavtal och andra överenskommelser gällande dataskydd, och förutsätter att verksamheten har identifierat samt registrerat personuppgiftsbiträden i registerförteckningen. Även verksamhetens rutiner för uppdatering och uppföljning av tecknade biträdesavtal innefattas.

#### ***Kontrollpunkt 5: Registerförteckning***

Kontrollpunkten avser verksamhetens efterlevnad av skyldigheten att systematiskt dokumentera alla personuppgiftsbehandlingar i form av ett register. Även verksamhetens arbete med, och rutin för, att säkerställa ett uppdaterat och heltäckande personuppgiftsregister innefattas.

#### ***Kontrollpunkt 6: Konsekvensbedömning/samråd***

Kontrollpunkten avser verksamhetens förutsättningar för att kunna identifiera när en konsekvensbedömning ska göras samt genomföra denna. Även verksamhetens rutiner för arbetet med konsekvensbedömningar samt hur dataskyddsombudet involveras i arbetet ingår. Därtill tillkommer verksamhetens rutin för att hantera de risker som identifieras i konsekvensbedömningen, samt hur genomförda konsekvensbedömningar följs upp och hålls aktuella.

#### ***Kontrollpunkt 7: Hantering av registrerades rättigheter***

Kontrollpunkten avser verksamhetens förutsättningar för att hantera de registrerades rättigheter, till exempel registerutdrag eller radering. En förutsättning för att verksamheten ska kunna hantera de registrerades rättigheter är att man har en process och rutiner för arbetet, så att den registrerades personuppgifter enkelt kan lokaliseras vid efterfrågan. Även verksamhetens rutin för att hantera ett tillbakadragande av samtycke ingår i kontrollpunkten

#### ***Kontrollpunkt 8: Kunskapsnivån i verksamheten***

Kontrollpunkten avser verksamhetens arbete med att utbilda och upprätthålla kunskapsnivån i dataskyddsfrågor hos anställda.

### **3.2 Fördjupad kontroll 2023**

Den fördjupade kontrollen utgår från verksamhetens specifika risker. För verksamhetsåret har följande punkter fastställts:

#### ***Fokusområde 1***

##### ***Kontrollpunkt 4: Personuppgiftsbiträdesavtal***

Den personuppgiftsansvarige är ansvarig för all behandling som utförs å dennes vägnar. En personuppgiftsansvarig som anlitar ett personuppgiftsbiträde att utföra personuppgiftsbehandlingar för sin räkning är alltså fortfarande personuppgiftsansvarig och kan inte avsäga sig de skyldigheter som följer av detta ansvar. Det är således av stor vikt att personuppgiftsansvariga har överblick över sina anlitade personuppgiftsbiträden och att de uppfyller de kvalitetskrav och krav vid, bl.a., anlåtande av underbiträden som uppställs i förordningen. Förordningen kräver även att förhållandet mellan den personuppgiftsansvarige och personuppgiftsbiträdet regleras genom avtal (eller annan rättsakt). Förordningen uppställer även vissa krav på

vad ett sådant avtal ska innehålla. Denna fördjupade kontroll syftar till att undersöka vilka som behandlar personuppgifter för Region Västerbottens räkning och ifall dessa förhållanden är reglerade genom adekvata avtal. För att skapa en överblick över Regionens generella och övergripande arbete med personuppgiftsbiträden inkluderar kontrollen även en undersökning av vilka rutiner och arbetssätt som Regionen har vid anlitan­de av personuppgiftsbiträden.

## **Fokusområde 2**

### **Kontrollpunkt 5: Registerförteckningen**

Registerförteckningen är ett krav enligt förordningen och ska kunna visas för tillsynsmyndigheten vid efterfrågan. I Regionen används i nuläget en sharepointlösning där verksamheterna registrerar sina behandlingar. Dataskyddsförordningen ställer krav på vad som ska förekomma i registret över personuppgiftsbehandlingar. Det handlar bland annat om ändamål för behandlingen, kategorier av registrerade och huruvida överföring av personuppgifter till tredjeland sker. Eftersom tillsynsmyndigheten kan begära att ta del av registret är det av yttersta vikt att verksamheten dokumenterar sina behandlingar korrekt i registret. Denna fördjupade kontroll avser undersöka Regionens dokumentation av personuppgiftsbehandlingarna för att säkerställa att de krav som förordningen ställer upp efterlevs.

## 4. Uppföljning

### 4.1 Uppföljning av lämnade rekommendationer

I dataskyddsförordningen anges att dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges högsta förvaltningsnivå, för att säkerställa att högsta ledningen är medveten om dataskyddsombudets råd och rekommendationer.

Detta är grunden för ett proaktivt arbetssätt och utgör en trygghet för nämnd/styrelse som uppmärksammas på status och observerade brister i dataskyddsarbetet. Det är då också av vikt för nämnd/styrelse att veta hur eventuella rekommendationer/brister omhändertagits. Dataskyddsombudet kommer därför årligen att följa upp hanteringen av de rekommendationer som lämnats till verksamheten och rapportera detta i årsrapporten.

#### 4.1.1 Uppföljning av hittills genomförda kontroller

Sedan dataskyddsförordningen trädde i kraft i maj 2018 har dataskyddsombudet genomfört kontroller 2019 och 2022 de brister som funnits kan genom åren sammanfattas i följande:

- Brister i att registerförteckna personuppgiftsbehandlingar
- Personuppgiftshandläggare har inte utsetts för samtliga verksamheter
- Kunskapsnivån bland medarbetarna om skyldigheten att rapportera personuppgiftsincidenter behöver höjas.

Dessa åtgärder kommer att följas upp inom ramen för de fasta kontrollpunkterna under 2023.

## 5. Rapportering

### 5.1 Delrapportering

Dataskyddsombudet kan komma att delrapportera större granskningar eller områden som behöver vidtas åtgärder kring skyndsamt utifrån de fokusområden som granskats. Genom en sådan delrapportering säkerställs att personuppgiftsansvarig nämnd/styrelse hålls informerad om dataskyddsombudets observationer av verksamhetens personuppgiftshantering. Formen för rapporteringen anpassas efter dataskyddsombudets bedömning av verksamhetens behov.

### 5.2 Årsrapport

Verksamhetens dataskyddsarbete kommer att sammanställas i en skriftlig årsrapport till nämnd/styrelse. Årsrapporten kommer innehålla information om genomförda kontroller, lämnade rekommendationer samt en övergripande bedömning av status på verksamhetens personuppgiftshantering utifrån fasta kontrollpunkter.

### 5.3 Särskilt yttrande till högsta ledning

Om det skulle uppstå situationer där den ansvarige fattar beslut som är oförenliga med den allmänna dataskyddsförordningen och dataskyddsombudets råd, till exempel om en allvarlig brist kvarstår och inte åtgärdas, har dataskyddsombudet



möjlighet att klargöra sin avvikande ståndpunkt genom ett yttrande riktat till högsta förvaltningsnivå och till dem som fattar besluten.

#### **5.4 Beslutanderätten i dataskyddsfrågor**

Beslutanderätten i dataskyddsfrågor ligger alltid på den personuppgiftsansvarige och aldrig på dataskyddsombudet. Dataskyddsombudet är en specialist med en rådgivande roll och är en resurs som, på ett oberoende sätt, fokuserar på dataskyddsfrågorna i verksamheten och på det sättet bistår den personuppgiftsansvarige med bedömningar och råd. Om nämnden/styrelsen väljer att inte följa dataskyddsombudets rekommendationer ska skälen till detta motiveras och dokumenteras i enlighet med god praxis samt för att uppfylla ansvarsskyldigheten. Detta är även viktigt för det fall att frågan senare skulle bli föremål för tillsyn

## **6. Kontakt**

Eventuella frågor och synpunkter hänvisas i första hand till dataskyddsombud, [dataskyddsombud@regionvasterbotten.se](mailto:dataskyddsombud@regionvasterbotten.se).

Umeå 19-12-2022