

# Dataskyddspolicy

## Syfte och ansvar

Syftet med denna policy är att säkerställa att RBU hanterar personuppgifter i enlighet med EU:s dataskyddsförordning (General Data Protection Regulation – GDPR).

Policyn omfattar alla behandlingar där personuppgifter hanteras och omfattar såväl strukturerad som ostrukturerad data.

RBU är personuppgiftsansvarig för de personuppgifter som behandlas av organisationen. Förbundsstyrelsen ansvarar för att behandlingen av personuppgifter följer denna policy. Kanslichefen ansvarar för att policyn implementeras och efterlevs i verksamheten, samt ansvarar för uppdatering av policyn till följd av nya och förändrade regelverk.

## Kunskap i organisationen

Samtliga anställda inom RBU ska ges grundläggande utbildning för att uppnå de kunskaper om dataskydd som krävs för att RBU ska kunna efterleva denna policy.

## Definition av personuppgifter

RBU behandlar ett stort antal personuppgifter i sin verksamhet. Personuppgifter är uppgifter som kan kopplas till en enskild person, antingen ensamt (som ett personnummer) eller tillsammans med andra personuppgifter (exempelvis ett förnamn och en bostadsadress). Begreppet personuppgift är brett och fångar alla typer av uppgifter som säger något om en person som identifierar personen. Exempel på vad som kan vara personuppgifter är namn, adress, telefonnummer, mailadress, medlemsnummer, bankkortsnummer, foto eller inspelning.

## Legal grund för behandling av personuppgifter

Behandling av personuppgift ska alltid vila på en legal grund för att vara tillåten enligt GDPR. De legala grunder som kan vara aktuella i RBU:s verksamhet är följande:

1. Samtycke - Den registrerade har sagt ja till personuppgiftsbehandlingen.
2. Avtal - Den registrerade har ett avtal eller ska ingå ett avtal med RBU.
3. Intresseavvägning - RBU får behandla personuppgifter utan den registrerades samtycke om RBU:s intressen väger tyngre än den registrerades och om behandlingen är nödvändig för det aktuella ändamålet.
4. Rättslig förpliktelse - Om det finns lagar eller regler som gör att RBU måste behandla vissa personuppgifter i sin verksamhet.

## Dokumentation av behandling av personuppgifter

RBU:s behandling av personuppgifter dokumenteras i ett särskilt dokument. Av dokumentet ska för varje typ av behandling framgå:

1. Vilken behandling som görs.
2. Vilken typ av personuppgifter som behandlas.
3. Behandlingens ändamål.
4. Legal grund för behandlingen.
5. Var personuppgifterna lagras.
6. När gallring av personuppgifter ska göras.
7. Eventuella personuppgiftsbiträdesavtal som omfattar uppgifterna.

### **Konsekvensbedömning**

Innan en ny personuppgiftsbehandling som innebär särskilda risker för de registrerade ska det göras en bedömning av vilka konsekvenser behandlingen kan få och vilka åtgärder som behövs för att minska riskerna.

### **Rutin vid personuppgiftsincident**

En personuppgiftsincident definieras som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas. Det kan också vara fråga om en personuppgiftsincident om en säkerhetsincident leder till obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna.

Om det inträffar en personuppgiftsincident, till exempel ett dataintrång eller en oavsiktlig förlust av uppgifter, ska RBU anmäla detta till Datainspektionen inom 72 timmar. Information om personuppgiftsincidenten ska även lämnas till de registrerade personerna.

### **Rutin vid registerutdrag**

Om någon begär ett registerutdrag över vilka personuppgifter som RBU lagrar avseende den egna personen ska samtliga register sökas igenom och eventuella uppgifter om personen skyndsamt lämnas ut till vederbörande.

### **Rutin vid begäran om radering av personuppgifter**

Om någon begär att personuppgifter som RBU lagrar avseende den egna personen ska raderas ska samtliga register sökas igenom och eventuella uppgifter om personen raderas. Detta gäller dock inte om RBU omfattas av ett lagligt krav att fortsatt behålla uppgiften, exempelvis bokföringsdata.

### **Hantering av leverantörer och personuppgiftsbiträden**

RBU:s krav på att personuppgifter hanteras i enlighet med GDPR ska alltid säkerställas vid upphandling och utveckling av IT-lösningar och tjänster, och ska vara en del i kravspecifikation och eventuella avtal. När leverantörer till RBU, som en del i avtalsförpliktelse, ska hantera personuppgifter som RBU lagrar ska ett personuppgiftsbiträdesavtal alltid upprättas.