



---

**ERIP AB**  
**STORA GATAN 42**  
**722 12 VÄSTERÅS**  
**SVERIGE**

info@erip.se  
www.erip.se

## **ERIP som tjänsteleverantör och den nya dataskyddsförordningen**

### **GDPR**

Den 25 maj 2018 träder den nya europeisk dataskyddsförordningen, "The General Data Protection Regulation (GDPR) i kraft.

Förordningen kommer att implementeras i alla lokala personuppgiftslagar inom hela EU och EES-regionen. Den kommer att gälla alla företag som säljer till och lagrar personuppgifter (Appendix 1) om medborgare i Europa, inklusive företag på andra kontinenter.

Det ger medborgarna i EU och EES större kontroll över sina personuppgifter och säkrar att informationen skyddas i hela Europa.

Det görs ingen skillnad mellan personuppgifter om individen i hans eller hennes privata, offentliga eller professionella roll – personen ses som en och samma individ oavsett roll. I en B2B-situation handlar dessutom allt om individer som interagerar och delar information med och om varandra. Kunder på B2B-marknader är så klart företag, men relationerna som hanterar de affärsmässiga relationerna är individer.

Villkoren för att erhålla samtycke är strängare enligt GDPR. Individen har rätten att återkalla samtycke när som helst och det måste ges separata samtycken för olika bearbetningsaktiviteter. Detta innebär att du måste kunna bevisa att individen har samtyckt till en viss åtgärd, till exempel att få ett nyhetsbrev. Det är inte tillåtet att förutsätta eller lägga till en ansvarsfriskrivning och det räcker inte att erbjuda möjligheten att tacka nej.

#### **Referens**

<https://www.datainspektionen.se/dataskyddsreformen/>

Enligt GDPR har individer bl.a. följande rättigheter när det gäller vilken information som samlas in om dem:

1. Varje behandling (Appendix 1) av personuppgifter måste ha en laglig grund. För att det ska vara tillåtet att behandla personuppgifter måste det alltid finnas ett stöd i dataskyddsförordningen, en så kallad laglig grund. En sådan laglig grund är samtycke från den registrerade.

#### 2. Rätt till tillgång

Detta ger individen rätt att få tillgång till sina personuppgifter och få veta hur dessa kommer att användas av företaget efter att de har blivit insamlade. På begäran av en individ är företaget tvunget att gratis och i elektroniskt format tillhandahålla en kopia av personuppgifterna.



### 3. Rätten att bli bortglömd

Om individen inte längre är kund eller vill återkalla det samtycke som har gett företaget rätt att använda personuppgifterna, har individen under vissa förutsättningar rätt att få sin information raderad.\*

### 4. Rätten till dataportabilitet

Individen har rätt att överföra sina data från en tjänsteleverantör till en annan. Och detta måste ske i ett vanligt och maskinläsbart format.

### 5. Rätten att bli informerad

Rätten för individen att bli informerad omfattar i princip alla typer av insamling av personuppgifter som företagen gör.

### 6. Rätten att få information korrigerad

Detta garanterar att individen kan få sina uppgifter uppdaterade om dessa är inaktuella eller felaktiga.

### 7. Rätten att begränsa behandling

Individen kan under vissa förutsättningar begära att dess uppgifter inte behandlas. Uppgifterna finns kvar, men dess användning begränsas.

### 8. Rätten att invända

Detta inkluderar rätten att avbryta behandling av personuppgifterna i syfte att använda dem för direkt marknadsföring. Det finns inga undantag till denna regel och all eventuell behandling i marknadsföringssyfte måste avbrytas så snart företaget får denna begäran. På samma sätt måste individen meddelas denna rättighet tydligt och klart i början av all kommunikation.

### 9. Rätten att meddelas

Om det har förekommit ett dataintrång som omfattar en individs personuppgifter, har individen i vissa fall rätt att få vetskap om detta inom skälig tid efter det att personuppgiftsbrottet blev känt.

### **Referens**

<https://www.datainspektionen.se/dataskyddsreformen/>



---

## Hur påverkas Erips tjänster?

Det är både nya rutiner och nya hjälpmedel som måste vara på plats avseende support och drift åt våra kunder för att vi ska kunna fullgöra våra förpliktelser som personuppgiftsbiträde (Appendix 1)

Som tjänsteleverantör är utmaningen således inbyggt systemstöd för integritet (Privacy by Design)

Säkerhetsmässigt säkerställer vi i samarbete med vår driftspartner att våra systems data är skyddat.

I nästa version som kommer inom kort kommer det finnas funktioner på plats där användaren har fullständig kontroll över sitt eget konto.



## **Appendix 1 Personuppgiftsbiträde**

Personuppgiftsbiträde är den som behandlar personuppgifter för en personuppgiftsansvarigs räkning. Ett personuppgiftsbiträde finns alltid utanför den personuppgiftsansvariges organisation. Ett personuppgiftsbiträde kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

De biträden som den personuppgiftsansvarige anlitar ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

Ett personuppgiftsbiträde och dess personal får enbart behandla personuppgifter enligt instruktion från den personuppgiftsansvarige. Biträdet får inte anlita ett annat biträde utan att i förhand få ett skriftligt tillstånd av den personuppgiftsansvarige.

En nyhet i förordningen är att några av de skyldigheter som tidigare har gällt för den personuppgiftsansvarige nu även gäller för personuppgiftsbiträdet, till exempel kraven på att föra register över behandlingar, att säkerställa en lämplig säkerhetsnivå och att i vissa fall utse ett dataskyddsombud.

Även personuppgiftsbiträdet kan bli föremål för tillsyn eller administrativa sanktionsavgifter och bli skadeståndsansvarig. Den personuppgiftsansvarige och personuppgiftsbiträdet måste upprätta ett så kallat biträdesavtal. Dataskyddsförordningen räknar upp vad ett sådant biträdesavtal ska innehålla.

### **Personuppgifter**

Varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

### **Behandling**

En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

### **Referens**

<https://www.datainspektionen.se/dataskyddsreformen/>