

# Integritetspolicy - övergripande

## 1 Syftet med denna policy

Alla individer vars personuppgifter behandlas inom ramen för Dipart Entreprenad AB verksamhet ska vara trygga med hur vi hanterar deras uppgifter.

Policyn beskriver på ett övergripande plan hur personuppgifter kan behandlas, för vilka syften och på vilket sätt av Dipart Entreprenad AB.

Denna policy ska säkerställa att Dipart Entreprenad AB:

- Följer gällande dataskyddslagstiftning, GDPR
- Lagrar och hanterar personuppgifter på ett korrekt och enhetligt sätt
- Kommunicerar tydligt och öppet gällande hur personuppgifter hanteras i verksamheten
- Kan tillmötesgå anställdas, kunders och andra intressenters rättigheter
- Skyddar den egna verksamheten mot hot och därmed minimerar integritetsrisker

## 2 Tillämpning, revidering

Denna policy är tillämplig för företagets styrelseledamöter, VD, medarbetare samt uppdragstagare som berörs av vår verksamhet.

Dipart Entreprenad AB krav på att personuppgifter hanteras enligt GDPR ska alltid säkerställas vid upphandling och utveckling av IT-lösningar och tjänster. Det ska vara en del i kravspecifikationen och eventuella avtal.

## 3 Organisation, ansvar

VD har det övergripande ansvaret för innehållet i denna policy samt att den implementeras och efterlevs av verksamheten. VD har delegerat ansvaret för till IT-chefen. IT-chefen är således ansvarig för att hålla policyn uppdaterad och att den efterlevs.

Alla medarbetare ansvarar för att de agerar i enlighet med denna policy och vad den vill säkerställa.

Följande personer har särskilt ansvar för delar av dataskyddsarbetet:

- Patrick Lepierre VD  
Ytterst ansvarig, delegerat ansvaret för efterlevnaden av denna policy till IT-chefen
- Jan Thorsell IT-chef  
Huvudansvarig för Diparts personuppgiftshantering.
- Elin Näverfelt HR-chef  
Hela anställningsprocessen, personalregistrering

Varje avdelning som hanterar personuppgifter i sin verksamhet måste säkerställa att uppgifterna behandlas i enlighet med denna policy samt följer kompletterande uppsatta instruktioner.

Ägare / Funktion	Skapat datum	Senast rev. / av	Ändringar	Plats
IT	2018-05-25	2021-12-28/JT	Större uppdatering av innehållet	HR

Var och en som arbetar inom ramen för Dipart Entreprenad AB verksamhet är skyldig att följa denna policy samt att samarbeta med ansvariga personer när det är relevant.

## 4 Viktiga begrepp och definitioner

Denna policy rör hantering av personuppgifter. Personuppgifter är all information som kan användas för att identifiera en enskild person, direkt eller indirekt. Begreppet personuppgifter inkluderar (men är inte begränsat till):

Direkta personuppgifter är framför allt namn, personnummer och information som direkt pekar ut en individ utan att man behöver tillföra ytterligare information. Exempel:

- Namn
- Personnummer
- E-postadress, ex [fornamn.efternamn@dipart.se](mailto:fornamn.efternamn@dipart.se)

Indirekta personuppgifter är uppgifter som pekar ut en individ om man kompletterar dem med annan information. Exempel:

- Telefonnummer
- IP-adress
- Kundnummer
- Bilder (på personer)

I uttrycket **behandling av personuppgifter** inkluderas allting som görs där personuppgifter förekommer, exempelvis administration av, kommunikation med och lagring av sådana uppgifter för olika ändamål och i olika sammanhang.

I den mån **känsliga personuppgifter** förekommer i Dipart Entreprenad AB verksamhet gäller särskilda regler för dessa. Känsliga personuppgifter är:

- Uppgifter som avslöjar ras eller etniskt ursprung,
- Uppgifter som avslöjar politiska åsikter,
- Uppgifter som avslöjar religiös eller filosofisk övertygelse,
- Uppgifter om medlemskap i fackförening,
- Uppgifter om hälsa,
- Uppgifter om sexualliv eller sexuell läggning,
- Genetiska uppgifter, och
- Biometriska uppgifter för att entydigt identifiera en fysisk person.

Observera att även uppgifter som indirekt avslöjar känslig information av detta slag inkluderas.

Dipart Entreprenad AB är **personuppgiftsansvarig** för de flesta av de personuppgiftsbehandlingar som förekommer i verksamheten. Med detta menas att organisationen är den juridiska person som är ytterst ansvarig för personuppgifterna, och som bestämmer över ändamål och medel. I specifika fall kan det vara så att någon annan än Dipart Entreprenad AB är personuppgiftsansvarig. Roller och ansvarsfördelning mellan organisationen och eventuella **personuppgiftsbiträden** ska framgå för varje behandling i registerförteckningen.

## 5 Ändamål med behandling av personuppgifter

Personuppgifter får bara samlas in för berättigade ändamål och mängden uppgifter ska begränsas till vad som är nödvändigt för ändamålen. Uppgifterna får inte senare behandlas på ett sätt som är oförenligt med dessa ändamål och inte heller sparas längre än nödvändigt.

Ägare / Funktion	Skapat datum	Senast rev. / av	Ändringar	Plats
IT	2018-05-25	2021-12-28/JT	Större uppdatering av innehållet	HR

Varje personuppgiftsbehandling ska ske enligt följande principer:

- Laglighet
- Ändamålsbegränsning
- Uppgiftsminimering
- Korrekthet
- Lagringsminimering
- Integritet och konfidentialitet

Det finns särskilda regler när det gäller hanteringen av känsliga personuppgifter. Utgångspunkten är att det är förbjudet att registrera känsliga personuppgifter. Det finns undantag från förbudet, bland annat för arbetsrättsliga syften, för att försvara ett rättsligt anspråk, eller om det finns ett tydligt och frivilligt samtycke från den registrerade. När det gäller hantering av känsliga personuppgifter så skall dessa särskilt skyddas.

## 6 Generella riktlinjer

### Utbildning

Alla tjänstemän ska få grundläggande dataskyddsutbildning, för att säkerställa förståelse för vikten av att hantera personuppgifter korrekt. Ansvarig för att utbildningen genomförs är IT-chefen.

Varje avdelning ansvarar för att berörda medarbetare får ta del av sådana instruktioner och rutiner som är relevanta för dem, och sådan information som behövs för att var och en ska kunna utföra sitt arbete i linje med dataskyddslagstiftningen. Detta inkluderar, men är inte begränsat till, utbildning av nyanställda.

### Registerförteckning

Detaljerad information om varje slags behandling av personuppgifter som förekommer i processer, IT-system och på olika avdelningar inom ramen för Dipart Entreprenad AB verksamhet ska finnas dokumenterad i organisationens registerförteckning. Förteckningen ska löpande hållas uppdaterad och fungera som ett heltäckande register över alla personuppgiftsbehandlingar, i enlighet med kraven i artikel 30 GDPR.

Registerförteckningen administreras av IT-chefen och HR-chef. System- och informationsägare samt avdelningsansvariga kan komma att tilldelas ansvar för specifika delar av registerförteckningen i samarbete med IT-chefen. Förteckningen kan visas upp för tillsynsmyndigheten på begäran.

### Rättslig grund

Varje behandling av personuppgifter ska ha en specificerad så kallad **rättslig grund** för att det ska vara lagligt att hantera personuppgifterna. Inga personuppgifter får behandlas hos Dipart Entreprenad AB utan att det finns en identifierad och lämplig rättslig grund. En godtagbar rättslig grund kan exempelvis vara ett avtal som ska uppfyllas, ett berättigat intresse, en laglig skyldighet (till exempel enligt bokföringslagen eller arkivlagen) eller ett faktiskt samtycke från de registrerade. Alla de olika möjliga rättsliga grunderna finns listade i artikel 6 GDPR.

Det är inte tillåtet att behandla känsliga personuppgifter förutom i specifika undantagsfall, som i så fall ska finnas beskrivna i registerförteckningen samt i kompletterande policydokument/rutinbeskrivningar.

Ägare / Funktion	Skapat datum	Senast rev. / av	Ändringar	Plats
IT	2018-05-25	2021-12-28/JT	Större uppdatering av innehållet	HR

De rättsliga grunder som vi på Dipart normalt använder är:

- 1, Samtycke: Den registrerade har lämnat sitt samtycke till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
- 2, Avtalsförhållande: Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
- 3, Rättslig förpliktelse: Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige. Ex: föra patientjournal, spara bokföringsmaterial, betala in källskatter
- 4, Berättigat intresse: Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

## Ändamålsbegränsning och uppgiftsminimering

Personuppgifter får endast behandlas för specifika syften, i den utsträckning de behövs och i enlighet med dataskyddslagstiftningen.

Endast sådana personuppgifter som faktiskt behövs får samlas in och sparas. Inga uppgifter får sparas med lösa motiveringar såsom att de "kanske kan vara bra att ha".

Behandling av personuppgifter i nya sammanhang (för nya ändamål) måste alltid på förhand utvärderas och kontrolleras med dataskyddsansvariga, för att säkerställa att den nya hanteringen inte riskerar att kränka de registrerade personernas integritet eller på annat sätt bryta mot dataskyddslagstiftningen.

## Behörighetsbegränsning

De personuppgifter som förekommer i verksamheten ska endast vara tillgängliga för personer som specifikt behöver dem i sitt arbete. För känsliga personuppgifter ska en snävare behörighetstilldelning generellt sett gälla än för mer harmlösa uppgifter.

## Lagringsminimering

Personuppgifter som inte längre behövs (och som man inte heller är skyldig att spara) ska gallras löpande. Observera att det kan finnas lagkrav på att arkivera och spara uppgifter, men det ska finnas gallringsrutiner för varje process och varje system där personuppgifter förekommer. Var och en som arbetar där är skyldig att följa dessa rutiner.

Personuppgifter får inte användas på annat sätt eller överföras till och/eller behandlas på annan plats (system/lagringsställe/enhet) än vad som följer av gällande rutiner och instruktioner.

Mer information i separat gallringspolicy.

## Information till registrerade

Alla vars personuppgifter hanteras av Dipart Entreprenad AB har rätt till information om hur deras personuppgifter hanteras. Detta gäller såväl anställda som kunder och andra grupper. Informationen ska vara lättillgänglig samt tillräckligt utförlig för att motsvara kraven i dataskyddslagstiftningen. Informationen ska lämnas på ett klart och tydligt sätt.

Informationen lämnas i huvudsak via intranätet (för anställda) och på den offentliga webbplatsen i form av en länk till denna integritetspolicy.

## De registrerades rättigheter

Dipart Entreprenad AB ska ha rutiner och instruktioner på plats för hur organisationen ska fullgöra sina skyldigheter gentemot de registrerade. De registrerades rättigheter framgår av 3

Ägare / Funktion	Skapat datum	Senast rev. / av	Ändringar	Plats
IT	2018-05-25	2021-12-28/JT	Större uppdatering av innehållet	HR

kapitlet i dataskyddsförordningen (artiklarna 12–23), och dessa rättigheter ska Dipart Entreprenad AB vara beredda att tillmötesgå i alla situationer där det krävs. Detta omfattar:

- *Rätten till information*  
Den enskilde har alltid rätt att få veta när, hur och varför hans eller hennes personuppgifter behandlas.
- *Rätten till tillgång - Registerutdrag*  
De enskilde har rätt till att få ta del av den information om dem som finns sparad hos en organisation. En person kan be att få ut ett så kallat registerutdrag, det vill säga en kopia på alla de uppgifter som organisationen har samlat på sig om honom eller henne.
- *Rätten till rättelse*  
Den enskilde kan kräva att de uppgifter som behandlas är korrekta. Därmed har den enskilde också rätt att få uppgifterna korrigerade eller kompletterade vid behov.
- *Rätten till radering – Rätten att bli glömd*  
Den enskilde har rätt att begära att personuppgifter ska tas bort.

Om det inte finns någon annan grund för behandlingen än samtycke eller om grunden är ett avtalsförhållande och det har avslutats, så har man rätt att begära att "bli glömd". Gäller ej då det finns annan laglig grund för att behandla uppgifterna.

- *Rätten till begränsning*  
Den enskilde har i vissa fall rätt att kräva att behandlingen av personuppgifter begränsas. Uppgifterna får då endast behandlas för vissa avgränsade syften.
- *Rätten till dataportabilitet*  
Den enskilde har rätt att på begäran få ut de uppgifter som finns registrerade i syfte att föra över dem och återanvända dem hos en annan part.
- *Rätten till invändningar*  
Den enskilde har i vissa fall rätt att invända mot den personuppgiftsansvariges behandling av hans eller hennes personuppgifter. Rätten att invända gäller när personuppgifter behandlas för att utföra en uppgift av allmänt intresse, som ett led i myndighetsutövning eller efter en intresseavvägning.
- *Rätten till att göra invändningar*  
De registrerade har rätt att invända mot att deras uppgifter används i syfte att skicka direktmarknadsföring samt att ifrågasätta rättslig grund för behandlingen.
- *Rätten att slippa beslut grundat på en automatisk handling*  
Om någon registrerad anser sig ha blivit förfördelad, så ska han eller hon kunna bestrida det automatiskt fattade beslutet och begära att en omprövning görs av en fysisk person.

## Lagring och informationssäkerhet

Alla personuppgifter som finns hos Dipart Entreprenad AB ska skyddas genom säkra servrar och andra lämpliga tekniska och organisatoriska säkerhetsåtgärder i enlighet med artikel 32 GDPR. Känsliga personuppgifter kräver generellt högre säkerhet än mer harmlösa uppgifter. Vidare specifikationer gällande informationssäkerhet inom Dipart Entreprenad AB finns i separat IT-policy/Informationssäkerhetspolicy.

## Biträdesavtal

Dipart Entreprenad AB anlitar endast personuppgiftsbiträden som garanterar lämpliga tekniska och organisatoriska åtgärder och på andra sätt kan ge garantier för att kraven i dataskyddsförordningen uppfylls också när en annan aktör behandlar personuppgifter för vår räkning. Det ska finnas skriftliga biträdesavtal med samtliga leverantörer och andra personuppgiftsbiträden. Dataskyddsansvarig ansvarar tillsammans med respektive

Ägare / Funktion	Skapat datum	Senast rev. / av	Ändringar	Plats
IT	2018-05-25	2021-12-28/JT	Större uppdatering av innehållet	HR

informationsägare för att kontrollera att biträdesavtal finns och speglar kraven i artikel 28 GDPR.

## Incidentrapportering

Var och en som upptäcker eller misstänker en incident som skulle kunna innebära en integritetsrisk, ska rapportera detta vidare till dataskyddsansvariga. En personuppgiftsincident kan vara allt ifrån att någon har tappat en mobiltelefon till en hackerattack där kundinformation och kontokortsinformation blivit stulna. Rutiner kring hantering av incidenter ansvarar IT-chefen för hos Dipart Entreprenad AB. Mer information finns i separat Informationssäkerhetspolicy.

## 7 Roller, ansvar och kontaktuppgifter

Följande personer har särskilt ansvar för delar av dataskyddsarbetet:

- Jan Thorsell – IT-chef  
Ansvarar för: Huvudansvarig för alla frågor gällande personuppgifter, GDPR
- Elin Näverfelt – HR-chef  
Ansvarar för: Hela anställningsprocessen

Varje avdelning som hanterar personuppgifter i sin verksamhet måste säkerställa att uppgifterna behandlas i enlighet med denna policy samt följer kompletterande uppsatta instruktioner.

Var och en som arbetar inom ramen för Dipart Entreprenad AB verksamhet är skyldig att följa denna policy samt att samarbeta med ansvariga personer när det är relevant.

## 8 Tillsynsmyndighet

Dipart Entreprenad AB har gjort bedömningen att ansvarig tillsynsmyndighet för verksamheten är Integritetsskyddsmyndigheten (IMY).

Enskilda personer som har klagomål gällande Dipart Entreprenad AB hantering av personuppgifter har rätt att kontakta IMY.

## 9 Kompletterande policyer och instruktioner

Vidare riktlinjer och instruktioner som rör Dipart Entreprenad AB personuppgiftsbehandling finns i följande policy-dokument:

- Informationssäkerhet
- Gallring
- Sociala medier och webbpublicering
- IT
- Mobiltelefoner tjänstemän
- Mobiltelefoner yrkesarbetare

## 10 Kontaktuppgifter (För alla frågor gällande Diparts personuppgiftshantering)

e-post: [gdpr@dipart.se](mailto:gdpr@dipart.se)

Diparts växel: 08-716 90 50

IT-Chef: 08-515 16 217

Ägare / Funktion	Skapat datum	Senast rev. / av	Ändringar	Plats
IT	2018-05-25	2021-12-28/JT	Större uppdatering av innehållet	HR