

Personuppgiftspolicy

Senast uppdaterad: 2026-05-26

Benderskoncernen ("Benders", "vi", "oss") värnar om din personliga integritet och hanterar personuppgifter i enlighet med gällande dataskyddslagstiftning, inklusive **EU:s dataskyddsförordning (GDPR)** och kompletterande svensk lag.

Denna policy beskriver hur vi samlar in, använder, lagrar och delar personuppgifter, samt vilka rättigheter du har.

1. Syfte

Syftet med denna personuppgiftspolicy är att säkerställa att bolag inom Benderskoncernen behandlar personuppgifter på ett **lagligt, korrekt och säkert sätt** i enlighet med EU:s dataskyddsförordning (GDPR) och kompletterande nationell lagstiftning.

Policyn ska ge vägledning till medarbetare och chefer i hur personuppgifter får samlas in, användas, delas, lagras och raderas inom verksamheten.

2. Tillämpningsområde

Denna policy gäller för:

- Samtliga medarbetare, praktikanter, konsulter och inhyrd personal
 - All behandling av personuppgifter som sker inom ramen för Benders verksamhet
 - Samtliga IT-system, manuella register och tredjepartstjänster där personuppgifter förekommer
-

3. Roller och ansvar

Personuppgiftsansvarig

Som huvudregel gäller att varje bolag inom koncernen är personuppgiftsansvarigt för den behandling som sker inom dess verksamhet. Vid användning av koncerngemensamma system och funktioner är det normalt det enskilda bolaget som bestämmer syftet med behandlingen som är ansvarigt för sina uppgifter. Om koncerngemensamma funktioner tillsammans med ett eller flera bolag gemensamt bestämmer ändamål och medel för

behandlingen, föreligger gemensamt personuppgiftsansvar i enlighet med artikel 26 GDPR.

Ledning och chefer

Ansvarar för att:

- Policyn är känd och efterlevs inom respektive ansvarsområde
- Tillräckliga resurser och rutiner finns på plats

Medarbetare

Varje medarbetare ansvarar för att:

- Följa denna policy och tillhörande instruktioner
- Endast behandla personuppgifter när det är nödvändigt för arbetsuppgiften
- Rapportera misstänkta personuppgiftsincidenter utan dröjsmål

4. Grundläggande principer

All behandling av personuppgifter ska ske i enlighet med följande principer:

- Laglighet, korrekthet och transparens
- Ändamålsbegränsning
- Uppgiftsminimering
- Lagringsminimering
- Integritet och konfidentialitet

5. Kategorier av personuppgifter

Inom verksamheten kan bland annat följande kategorier av personuppgifter behandlas:

- Personnummer
- Information om anhöriga ("närmast anhörig", barn)
- Kontaktuppgifter (namn, adress, e-post, telefonnummer)
- Information som relaterar till medarbetas hälsa/mående (sjukfrånvaro, hälsoundersökningar, medarbetarsamtal etc)
- Löneuppgifter (Bankuppgifter, Skatteuppgifter)
- Pension- och försäkringsinformation
- Medlemskap i fackförening
- Tekniska uppgifter (IP-adress, loggar, enhetsinformation)
- Användnings- och beteendedata från webb och digitala tjänster
- Uppgifter i rekryteringsprocesser
- Kamerabevakningsmaterial

Endast personuppgifter som är nödvändiga för ett definierat ändamål skall behandlas.

6. Ändamål och rättslig grund

Personuppgifter får endast behandlas för:

- Avtal och affärsrelationer
- Kommunikation och service
- Personalrelaterat arbete
- Drift, säkerhet och förbättring av IT-system och webbplatser
- Rekrytering
- Säkerhet och skydd av medarbetare, besökare och tillgångar
- Uppfyllande av rättsliga förpliktelser

Behandlingen ska alltid stödjas av en giltig rättslig grund, såsom avtal, samtycke, rättslig förpliktelse eller berättigat intresse.

7. Delning och personuppgiftsbiträden

Personuppgifter får endast delas med:

- Inom bolaget som är personuppgiftsansvarigt i enlighet med dokumenterat syfte och övriga ramar
- Koncernbolag när det är nödvändigt
- Leverantörer som agerar personuppgiftsbiträden och omfattas av personuppgiftsbiträdesavtal
- Myndigheter när detta krävs enligt lag

Vid överföring av personuppgifter utanför EU/EES ska godkända skyddsåtgärder användas.

8. Lagring och gallring

Personuppgifter ska:

- Inte lagras längre än nödvändigt
- Gallras eller anonymiseras enligt fastställda rutiner
- Hanteras i enlighet med gällande lagkrav och interna beslut

Gallringstider skall alltid definieras per registrering av personuppgifter. Detta skall dokumenteras i Benders registerförteckning över insamlingen av samtliga personuppgifter till olika källor/platser/system.

9. Registrerades rättigheter

Benders ska alltid säkerställa att registrerades rättigheter enligt GDPR kan tillgodoses, vi skall kunna hantera begäranden inom de juridiska begrepp som GDPR omfattar. Se nedan lista för vilka dessa begrepp/områden är samt ett konkret exempel.

- Information - "Varför har ni mina uppgifter?"
- Tillgång - "Vilka uppgifter har ni om mig? Jag vill ha ett registerutdrag"
- Rättelse - "Ni har fel adress/telefonnummer, vänligen rätta till det"
- Radering - "Jag vill att ni raderar alla mina uppgifter"
- Begränsning - "Ni får inte använda mina uppgifter tills detta är utrett"
- Invändning - "Jag vill inte att ni använder mina uppgifter för marknadsföring"
- Dataportabilitet - "Jag vill ha min data så jag kan flytta till annan leverantör"

Begäranden ska hanteras skyndsamt enligt gällande lagstiftning.

10. Informationssäkerhet

Lämpliga tekniska och organisatoriska åtgärder ska vidtas för att skydda personuppgifter, tex:

- Behörighetsstyrning/Åtkomstkontroller
 - Loggning
 - Säkerhetskopiering
 - Incidenthantering
-

11. Personuppgiftsincidenter

Misstänkta eller konstaterade personuppgiftsincidenter ska omedelbart rapporteras enligt gällande incidenthanteringsrutin, i första hand kontaktas Benders Dataskyddsombud (se kontaktuppgifter nedan). Incidenter ska dokumenteras och, vid behov, anmälas till tillsynsmyndighet.

Telefon: 010-88 800 00

E-post: data.protection@benders.se

12. Uppföljning och efterlevnad

Efterlevnaden av hantering av personuppgifter görs regelbundet av den funktion/bolag som är ansvarig för registreringen. Policyn som helhet ses över vid behov, tex vid större förändringar i verksamhet eller förändrad lagstiftning. Datumet längst upp i policyn anger senaste uppdatering.