

# Bilaga 1 – Hantering av personuppgifter

## Hantering av personuppgifter

Följande instruktioner gäller för behandling av Personuppgifter av Leverantören, både i egenskap av personuppgiftsansvarig och i egenskap av personuppgiftsbiträde enligt med personuppgiftsbiträdesavtalet. Utöver vad som redan framgår av Personuppgiftsbiträdesavtalet ska Leverantören följa nedanstående instruktioner

<b>Ändamål</b>	Behandlingen av personuppgifter sker hos Leverantören såsom personuppgiftsansvarig, och i vissa fall där Leverantören är personuppgiftsbiträde, i syfte att leverera, utveckla, förvalta, felsöka, underhålla och administrera Leverantörens tjänster till och avtalsförhållande med Kunden.
<b>Kategorier av Personuppgifter</b>	I egenskap av personuppgiftsansvarig behandlas uppgifter som t.ex. namn, e-post, personnummer, adress, telefonnummer och liknande kontaktinformation till kund. Leverantören behandlar också till viss del användarnamn och IP-adresser.  I egenskap av personuppgiftsbiträde kan ytterligare kategorier förekomma (regleras då av personuppgiftsansvarige).
<b>Kategorier av Registrerade</b>	I egenskap av personuppgiftsansvarig behandlas information om kunder, leverantörer och partners till Leverantören. I egenskap av personuppgiftsbiträde kan ytterligare kategorier förekomma (regleras då av personuppgiftsansvarige).
<b>Gallringstid</b>	Personuppgifter som lagras direkt i våra system gallras eller anonymiseras inom skälig tid efter att Kund helt avslutat sin tjänst och våra kontraktuella åtagande upphört, eller om Kund valt att aktivt kräva borttagning av sina uppgifter. Undantag är data som har lagkrav att sparas längre (t.ex. finansiell information för Skatteverket eller bokföringsinformation) och dessa sparas då så länge vi har lagkrav på att spara informationen.  Information som lagras indirekt på våra tjänster, som t.ex. backuper av Kunds data, loggar eller liknande, specificeras på webbsida och/eller i avtal/villkor och sparas mellan 7 dagar och 12 månader beroende på tjänst.
<b>Praktisk hantering</b>	Insamling av uppgifter i egenskap av personuppgiftsansvarig sker vid registrering av Kunden via webbsida, och då också godkännande av villkor. Kundens information används för att identifiera Kund (både manuellt och automatiskt) för t.ex. utskick av fakturor och vid kommunikation med support. Vid beställning av tredjepartstjänster som t.ex. domäner eller SSL-certifikat skickas den information som krävs till tredje part. Detta förtydligas också i separata avtalsvillkor för domännamn.  IP-adresser och användarnamn behandlas också i form av loggning, monitorering och backup.  Behandlingar som utförs från Leverantören i rollen personuppgiftsbiträde utgörs normalt av exempelvis loggning, felsökning, monitorering, backup och kundtjänst/support.

## Tekniska och organisatoriska säkerhetsåtgärder

Nedan listar de åtgärder som tas från Leverantören i egenskap av personuppgiftsansvarig och personuppgiftsbiträde för att säkerställa att personuppgifterna behandlas på ett säkert vis.

<b>Privacy-by-design</b>	Utvecklingsprocesser och mjukvara från Leverantör tas fram med rutiner och processer som utgår från ett inbyggt dataskydd
<b>Fysiskt skydd</b>	Utrymmen där personuppgifter förvaras, så som serverhallar & kontor, ska skyddas genom lämpliga tillträdeskontroller för att säkerställa att endast behörig personal får tillträde.
<b>Skydd mot skadlig kod</b>	Relevanta system ska vara skyddade mot virus, trojaner och andra former av digitala intrång.
<b>Begränsning av access</b>	Inloggningar och accesser är rollbaserade och individbaserade, och grunden är att personal och system inte har mer access än nödvändigt för att utföra uppgiften.
<b>Backup</b>	Leverantören har backuper både på system där denne behandlar personuppgifter i egenskap av personuppgiftsansvarig, och där våra kunder behandlar personuppgifter.
<b>Loggning</b>	Leverantören har fullgod loggning kring access och ändring av personuppgifter
<b>Kryptering</b>	All kommunikation på över internet mellan system som hanterar personuppgifter sker krypterat
<b>Riskbedömning</b>	Leverantören utför löpande riskanalyser kring våra system och våra tjänster
<b>Processer och rutiner</b>	Leverantören har tydliga processer och rutiner för de olika typer av behandlingar som utförs.
<b>Systemregister</b>	Leverantören har fullgoda hjälpmedel för att få en bra kontroll på de system, enheter och organisationer som behandlar personuppgifter.
<b>Certifieringar</b>	Leverantören är certifierad enligt både ISO 9001 (Kvalitet) och ISO 27001 (Informationssäkerhet)