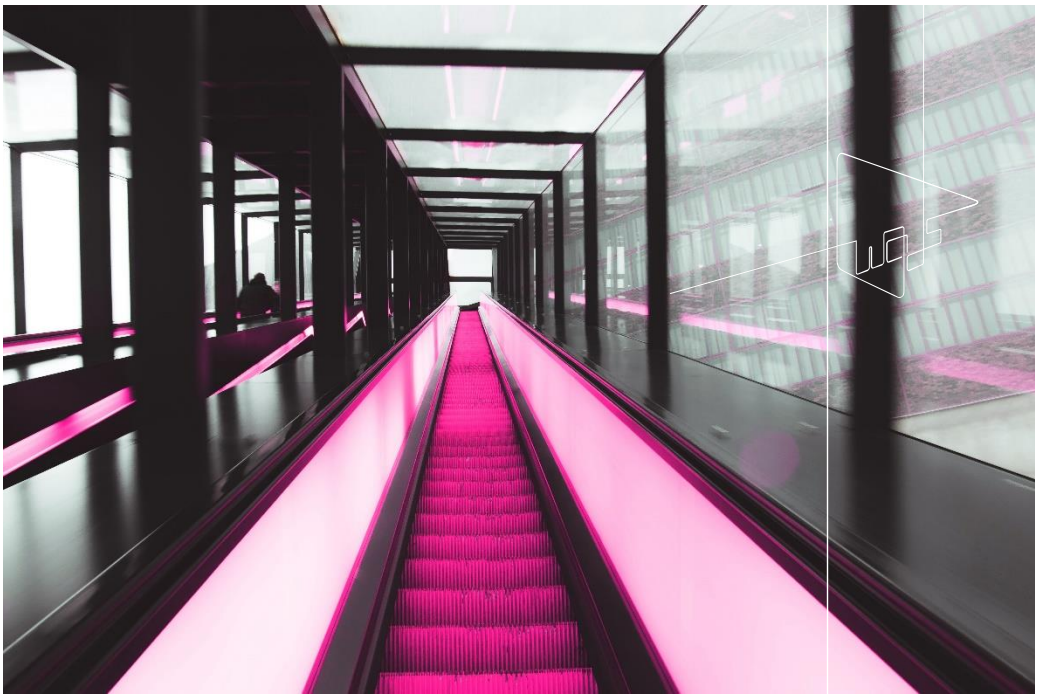


ways
simplifies document management

Informationssäkerhet personuppgifter - Ways Sweden

Detta dokument beskriver Ways Sweden ABs hantering av personuppgifter och känslig information.

INNEHÅLLSFÖRTECKNING

1. Ways behandling av personuppgifter

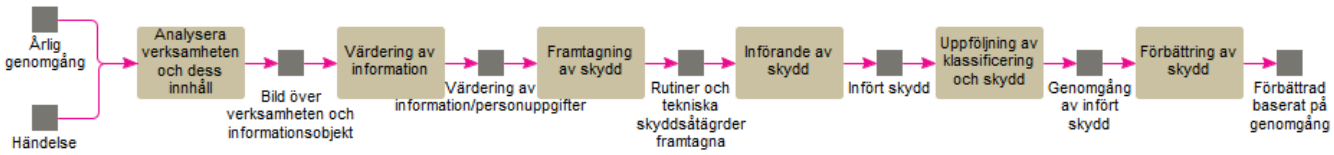
Ways har en kontinuitetsplan för hantering av personuppgifter.

Ways hanterar följande områden avseende persondata:

- Personuppgifter avseende anställda i Ways Sweden AB
- Kunduppgifter i marknadsföringssyfte i CRM
- Personuppgifter i applikationen MetaShare används enbart för faktureringsrutiner och tekniska kontaktuppgifter
- Indirekt access till kunddata för i de fall vi har drift och supportåtagande mot kund

1.1. Kontinuitetsplan

Ways arbetar med en kontinuitetsplan som syftar till att planera, genomföra, följa upp och förbättra vårt system för informationssäkerhet och GDPR enligt ISO/IEC 27001. Detta enligt nedanstående processbild:



2. Skyddet för personuppgifter

Ways målsättning är att värna skyddet för den personliga integriteten och att vidta alla de tekniska och organisatoriska åtgärder som krävs för att skydda personuppgifterna och säkerställa att behandlingarna sker i enlighet med gällande dataskyddslagstiftning och interna riktlinjer, policyer och rutiner för hantering av personuppgifter. Det innebär att endast de personer som behöver ha tillgång till uppgifterna, för att utföra sina arbetsuppgifter, skall ha tillgång till dem.

3. Säkerhetsåtgärder

Ways vidtar lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken och för att skydda de personuppgifter som vi behandlar mot personuppgiftsincidenter. Endast den personal hos Ways, som behöver tillgång till personuppgifterna, för att utföra uppdraget, har tillgång till dem. De är vidare skyldiga att iaktta sekretess som inte är mindre omfattande än det sekretessåtagande som följer av uppdragsavtalet.

För det fall en personuppgiftsincident inträffar kommer Ways, så snart Ways fått kännedom om den, att utan onödigt dröjsmål, skriftligen underrätta berörd part. Ways kommer i samband därmed och så snart

som möjligt att tillhandahålla en beskrivning av personuppgiftsincidenten samt en beskrivning av de åtgärder som vi, i förekommande fall, redan har vidtagit eller avser att vidta för att åtgärda personuppgiftsincidenten och/eller för att begränsa dess eventuella negativa effekter.

4. Tekniska och organisatoriska säkerhetsåtgärder

4.1. Dokumenthantering

Ways har en separat policy och rutin för dokumenthantering för att bevara en hög säkert avseende dokument.

4.2. Personalsäkerhet

I den utsträckning svensk lagstiftning tillåter utförs bakgrundskontroll av all personal före anställning. Detsamma gäller för personal som tillhandahålls av tredje part.

All ny personal informeras om sitt säkerhetsansvar och bekräftar skriftligen att de förbinder sig att följa alla tillämpliga riktlinjer och rutiner samt Ways krav på sekretessplikt.

En gång per år genomgår alla anställda och konsulter ett program för säkerhetsmedvetande samt en säkerhetsutbildning.

4.3. Drift- och kommunikationssäkerhet

Ändamålsenliga brandväggar finns, liksom rutiner för uppföljning av loggar.

Alla persondatorer är utrustade med hårddiskkryptering enligt senaste standard, lösenordskyddade skärmsläckare, personliga brandväggar, antivirusprogramvara och VPN. Även patchningsrutiner finns.

Endast Ways utrustning kan få åtkomst till Ways nätverk.

Lösningar för säker delning av information med kunder finns tillgängliga. Ways förbjuder lagring av företagsinformation i tjänster som Dropbox, Box, Google Drive, etc.

4.4. Styrning av åtkomst

Åtkomst till information baseras på användarens roll och ansvar. Behörighet ges utifrån principen att endast den som behöver tillgång till informationen, för att utföra en arbetsuppgift inom ramen för ett uppdrag, får tillgång till den. Alla användarkonton är hänförliga till en enskild individ.

Beslut om åtkomst fattas av informationsägaren.

Ways har rutiner för att lägga till, ändra och ta bort användarkonton samt för att ändra logisk access när arbetsuppgifter förändras. Inaktiva användarkonton spärras med automatik. Vidare finns rutin för att dra tillbaka fysisk och logisk access för personal och konsulter som slutar vid Ways.

Antalet användarkonton med höga behörigheter, som systemadministratör och motsvarande, har nedbringats till ett minimum. Personal med tillgång till sådana användarkonton använder separata konton när de utför normala arbetsuppgifter.

Systemstöd tillämpas för tvingande lösenordsbyten, krav på lösenordsstruktur samt utelåsning efter misslyckade åtkomstförsök.

4.5. Fysisk och miljörelaterad säkerhet

Serverlokaler är ändamålsenligt skyddade mot intrång, stöld, brand, vattenskador, strömavbrott och andra faror. Fysisk åtkomst till serverlokaler har begränsats till ett minimum av personal.

Ways har en Clean Desk Policy.

Säkra behållare finns för omhändertagande av känslig pappersdokumentation.

5. Incidenthantering

Ways har en incidenthanteringsprocess. Processen hanterar frågor så som vem som ansvarar för vad, vad ansvaret innebär samt hur rapportering, klassificering och eskalering ska ske. Skulle en incident bestå i att lagar, regler eller avtalsförpliktelser har åsidosatts, finns risk- och/eller skadereducerande rutiner, samt rutiner för utredning och, i förekommande fall, för rapportering till kunder och tillsynsmyndighet. I Ways obligatoriska utbildning inom säkerhetsområdet ingår hur en säkerhetsöverträdelse eller incident (inklusive personuppgiftsincident) ska identifieras och vem/vilka som i så fall ska kontaktas.

Vid personuppgiftsincident som medför risker för enskildas fri- och rättigheter hanteras dessa enligt följande:

1. Registrering av ett personuppgiftsärende
2. Rapportering till tillsynsmyndigheten inom 72 timmar
3. Rapportering till individ

Ways Sweden AB
Stockholm, 2023-01-27