

Policy för PS Olje AB rörande personuppgiftshantering

Innehållsförteckning

- 1 Inledning och syfte
- 2 Tillämpning och revidering
- 3 Organisation och ansvar
- 4 Begrepp och förkortningar
- 5 Personuppgiftsbehandling

1 INLEDNING OCH SYFTE

Syftet med denna policy är att säkerställa att PS Olje AB hanterar personuppgifter i enlighet med EUs dataskyddsförordning (General Data Protection Regulation – GDPR). Policyn omfattar alla behandlingar där personuppgifter hanteras och omfattar såväl strukturerad som ostrukturerad data.

Denna policy är förankrad hos alla våra medarbetare.

2 TILLÄMPNING OCH REVIDERING

Styrelsen ansvarar för att behandlingen av personuppgifter följer denna policy.

Policyn ska fastställas av styrelsen minst en gång per år och uppdateras vid behov.

VD är ansvarig för att hålla i processen kring årlig uppdatering av policyn till följd av nya och förändrade regelverk.

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

3 ORGANISATION OCH ANSVAR

Styrelsen har det övergripande ansvaret för innehållet i denna policy samt att den implementeras och efterlevs av verksamheten. Styrelsen får delegera ansvaret och implementationen till lämplig person på företaget.

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

4 BEGREPP OCH FÖRKORTNINGAR

Begrepp	Betydelse
Personuppgift	En personuppgift är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.
Registrerad	Den som en personuppgift avser, det vill säga den fysiska person som direkt eller indirekt kan identifieras genom personuppgifterna i ett register.
Personuppgiftsbehandling	En åtgärd eller kombination av åtgärder beträffande personuppgifter – oberoende av om de utförs automatiserat eller ej – såsom insamling, registrering, organisering och strukturering.

5 PERSONUPPGIFTSBEHANDLING

- Varje personuppgiftsbehandling ska ske enligt följande principer:

- Laglighet
 - Ändamålsbegränsning
 - Uppgiftsminimering
 - Korrekthet
 - Lagringsminimering
 - Integritet och konfidentialitet
- Vi lutar oss mot regeln i GDPR att vi har grund för personuppgiftsbehandling när personuppgiftsbehandlingen är nödvändig för att fullgöra ett avtal med den registrerade. Så vi sparar bara den information som behövs för att leverera varor och sköta fakturering och bokföring samt för att kunna informera om erbjudanden.
 - För mailhantering internt och externt har vi infört regler som skall säkerställa att personuppgifter i mail hanteras i enlighet med GDPR.
 - Vi lagrar aldrig uppgifter längre än nödvändigt med hänsyn till ändamålen med behandlingen. Vi genomför därför regelbundna gallringar bland lagrade personuppgifter och tar bort de uppgifter som inte längre behövs efter det att kundrelationen upphört. Vi kan dock behöva lagra personuppgifterna efter det att kundrelationen upphört, bland annat för att administrera eventuella garantier och reklamationsfrister, hantera rättsliga krav som kan tänkas riktas mot oss eller för att marknadsföra tjänster och skicka erbjudanden som vi tror kan vara av intresse för t.ex. våra f.d. kunder. Undantagsvis sparas därför personuppgifter viss tid efter kundförhållandets upphörande eller tills att personen invänt mot direktmarknadsföring. Personuppgifter avseende företrädare för potentiella kunder tas bort när dialogen med kunden upphört, under förutsättning att ingen kundrelation inletts, eller direkt om personen invänder mot direktmarknadsföring. Personuppgifter kan också mer generellt behöva lagras för att säkerställa uppfyllelse av legala skyldigheter, exempelvis avseende bokföring. Om sådan skyldighet föreligger kan personuppgifterna sparas i upp till 7 år.
 - Uppföljning och utvärdering av vår hantering av personuppgifter ska ske minst årligen.
 - Eventuella incidenter rörande personuppgifter som vi behandlar ska utan dröjsmål rapporteras till VD. VD ska utan onödigt dröjsmål och senast inom 72 timmar anmäla incidenten till Datainspektionen samt i övrigt vidta nödvändiga åtgärder med anledning av incidenten.
 - Våra krav på att personuppgifter hanteras enligt GDPR ska alltid säkerställas vid upphandling och utveckling av IT-lösningar och tjänster, och ska vara en del i kravspecifikationen och eventuella avtal.
 - Vi har vidtagit tekniska och organisatoriska åtgärder för att säkerställa en rimlig säkerhetsnivå som är lämplig för att skydda de personuppgifter som behandlas mot oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande av eller obehörig åtkomst till de personuppgifter som behandlas.