GDPR – Integritetspolicy Norrköping 2019-10-17

Behandling av personuppgifter på Exiso AB BESLUTADES AV LEDNINGEN

EXISO AB behandlar personuppgifter i enlighet med EU:s dataskyddsförordning GDPR (General Data Protection Regulation).

För att det ska vara tillåtet att behandla personuppgifter krävs en rättslig grund. I policyn nedan beskrivs hur EXISO AB (55….-….) samlar in, lagrar, använder och lämnar ut dina personuppgifter.

Vi på EXISO AB är måna om att vara helt transparenta med hur vi arbetar och hur vi hanterar dina personuppgifter. Här berättar vi hur och varför vi behandlar personuppgifter, inklusive cookies, samt dina rättigheter och våra skyldigheter gentemot dig, som vår eller kund, anställd eller besökare.

Vid frågor kring detta är du alltid välkommen att kontakta oss via info@exiso.se

För dig som är kund, anställd eller besökare

För oss på Exiso AB är personlig integritet viktigt. Vi eftersträvar en hög nivå av dataskydd. I denna policy förklarar vi hur vi samlar in och använder personuppgifter om dig som anställd. Vi beskriver också dina rättigheter och hur du kan göra dem gällande.

Du är alltid välkommen att kontakta oss om du har frågor om hur vi behandlar dina personuppgifter. Kontaktuppgifter står sist i denna text.

Vad är en personuppgift och vad är en behandling av personuppgifter?

Personuppgifter är alla uppgifter om en levande fysisk person som direkt eller indirekt kan kopplas till den personen. Det handlar inte bara om namn och personnummer utan även om till exempel bilder och e-postadresser.

Behandling av personuppgifter är allt som sker med personuppgifterna i IT-systemen, oavsett om det handlar om mobila enheter eller datorer. Det handlar om till exempel insamling, registrering, strukturering, lagring, bearbetning och överföring. I vissa fall kan även manuella register omfattas.

Personuppgiftsansvarig

För de behandlingar som sker inom Exiso AB:s verksamhet är Exiso AB personuppgiftsansvarig.

Vilka personuppgifter samlar vi in om dig och varför?

Vi behandlar i huvudsak namn, personnummer, organisationsnummer (gäller enskild firma), adress och kontaktuppgifter, bankkonto för löneutbetalning, fakturering. (Även uppgifter som du gett om närmast anhörig – gäller anställda).

Vi behandlar dina personuppgifter för att kunna fullgöra våra skyldigheter enligt avtal med dig och för att uppfylla regler i lag och även kollektivavtal.

Personuppgiftsbiträden

I en del situationer är det nödvändigt för oss att anlita andra parter. Till exempel olika IT-leverantörer för HR-system eller elektroniska körjournaler. De är då personuppgiftsbiträden till oss. Vi kontrollerar personuppgiftsbiträden för att säkerställa att de garanterar säkerheten och sekretessen för personuppgifterna. När personuppgiftsbiträden anlitas sker det bara för de ändamål som är förenliga med de ändamål vi själva har för behandlingen.

Aktörer som är självständigt personuppgiftsansvariga

Vi delar även dina personuppgifter med vissa andra aktörer som är självständigt personuppgiftsansvariga, till exempel myndigheter som Skatteverket, när vi är skyldiga att lämna ut sådana uppgifter med stöd av lag eller myndighetsbeslut. När dina personuppgifter delas med en aktör som är självständigt personuppgiftsansvarig gäller den organisationens integritetspolicy och personuppgiftshantering.

Hur länge sparar vi dina personuppgifter?

Vi sparar aldrig dina personuppgifter längre än vad som är nödvändigt för respektive ändamål. Vissa uppgifter i bokföringen behöver på grund av lagstiftning till exempel sparas minst sju år.

Vad är dina rättigheter som registrerad?

Som registrerad har du enligt gällande lagstiftning ett antal rättigheter. Du har rätt till att få ett utdrag som visar vilka personuppgifter vi har registrerade om dig. Du kan begära rättelse av felaktiga uppgifter och i vissa fall radering.

Kontakta oss vid frågor om hur vi behandlar personuppgifter.

Om du har frågor om hur vi behandlar personuppgifter kontakta Giota Christoforidou eller Robert Stipesevic som är ansvarig för personuppgiftsfrågor.

Personuppgiftsbehandling

Vad är en personuppgift?

Personuppgifter är all slags information som kan kopplas till en levande person, t ex namn, adress och personnummer. Även foton i de fall personen på fotot kan kännas igen. Registreringsnumret på en bil kan också vara en personuppgift om det går att sammankoppla registreringsnumret med en enskild person.

I dataskyddsförordningen skiljer man på ”vanliga” personuppgifter och känsliga personuppgifter.

Känsliga personuppgifter är:

* Hälsa, etniskt ursprung, politiska åsikter och sexuell läggning

Huvudregeln är att dessa uppgifter inte får behandlas. Dock finns det vissa undantag om den som personuppgiften handlar om har gett sitt samtycke eller om det är klart motiverat med hänsyn till ändamålet, vikten av en säker identifiering eller annat beaktansvärt skäl.

Eftersom känsliga personuppgifter anses ha ett större skyddsvärde än andra personuppgifter ställs det högre krav på att dessa uppgifter ges ett mer omfattande skydd.

Vad innebär behandling av personuppgifter?

Behandling av personuppgift är all hantering av personuppgifter, manuellt som elektroniskt.

För behandling behöver vi ha en laglig grund.

För att få behandla personuppgifter måste det finnas en laglig grund för behandlingen. För vår typ av verksamhet är det i första hand följande grunder som är aktuella:

* Rättslig förpliktelse – leva upp till lagar och regler exempelvis bokföringsskyldighet i bokföringslagen eller kraven på ett systematiskt arbetsmiljöarbete.

* Avtal – uppfylla ett avtal exempelvis anställningsavtal, kundavtal och leverantörsavtal.

* Intresseavvägning – nödvändig behandling för ett aktuellt ändamål där företagets intressen väger tyngre än den registrerades.

* Samtycke – den registrerade samtycker till behandlingen, kräver att den registrerade får tydlig information om vilka uppgifter som samlas in och vad de ska användas till.

I Dataskyddsförordningen finns det ett antal grundprinciper som alltid måste följas. EXISO AB följer samtliga grundprinciperna (se nedan)

Principerna innebär bland annat att vi:

* Måste ha stöd i Dataskyddsförordningen för att få behandla personuppgifter

* Får bara samla in personuppgifter för specifika, särskilt angivna och berättigade ändamål.

* Ska inte behandla fler personuppgifter än vad som behövs för ändamålen

* Ska se till att personuppgifterna är riktiga och att vi raderar dem när de inte längre behövs.

* Ska skydda personuppgifterna så att obehöriga inte får tillgång till dem eller att de förloras eller förstörs.

* Ska kunna redovisa att vi lever upp till Dataskyddsförordningen.

Personuppgiftsansvarig och personuppgiftsbiträde

Den som behandlar personuppgifter är antingen personuppgiftsansvarig eller personuppgiftsbiträde. Personuppgiftsansvarig är den som bestämmer för vilka ändamål uppgifterna ska behandlas och hur behandlingen ska gå till. Personuppgiftsbiträde är den som behandlar personuppgifter åt personuppgiftsansvarig. Båda dessa kan vara en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ.

Exiso AB är personuppgiftsansvarig för de behandlingar som görs inom företaget och för de som är personuppgiftsbiträden åt Exiso AB tecknas biträdesavtal som binder dem till att följa lagens krav.

Föra register över behandling

Både personuppgiftsansvariga och personuppgiftsbiträden är skyldiga att föra ett register eller en förteckning över behandlingar av personuppgifter. Dessa register ska finnas digitalt och på begäran ska registret kunna göras tillgängligt för Datainspektionen. Registret ska bland annat ge information om vilka personuppgifter som behandlas, ändamålet med behandlingarna och kontaktuppgifter till den som är ansvarig för behandlingen.

Informationssäkerhet

Rätt information ska finnas tillgänglig för rätt personer, och i rätt tid. Informationssäkerhet handlar framför allt om att förhindra information från att läcka ut, förvanskas, förstöras eller hamna i orätta händer och missbrukas.

För att kunna ha kontroll över de behandlingar som sker inom företaget är det därför mycket viktigt att endast de verktyg och lagringsytor som är godkända av företaget används.

De registrerades rättigheter

De personer vars personuppgifter behandlas, de registrerade, har ett antal rättigheter enligt Dataskyddsförordningen som i korthet innebär:

* Rätt att få information om när och hur deras uppgifter behandlas samt ha kontroll över dem

* Under vissa omständigheter kunna få sina uppgifter rättade, raderade eller blockerade, eller få ut eller flytta sina uppgifter.

ATT UPPDATERA SINA UPPGIFTER

För att uppdatera dina personuppgifter behöver du bara mejla oss på: info@exiso.se så kommer vi att uppdatera dina uppgifter.

ATT BLI GLÖMD

För att få dina uppgifter raderade ur våra system och register anmäler du det till oss på info@exiso.se

ATT FÅ DINA UPPGIFTER UTLÄMNADE OCH/ELLER EXPORTERADE

För att få veta vilka personuppgifter vi har lagrade om dig och för att eventuellt exportera dem till en ny leverantör anmäler du detta till oss på info@exiso.se. Vi skickar då snarast alla personuppgifter vi har lagrade till dig.

TREDJEPARTSINFORMATION

EXISO AB kan komma att lämna ut dina uppgifter till tredje part såsom samarbetspartners samt leverantörer av betal- och kommunikationstjänster. Tredje part får endast använda uppgifter för att kommunicera och eller sälja EXISO ABs tjänster. Uppgifter kan även komma för att lämnas ut för att följa EXISO ABs rättsliga intressen vid t.ex bedrägeri eller liknande.

Personuppgifterna kan komma att lämnas över till land utanför EU/EES om någon/några av våra samarbetspartners befinner sig där. Om så är fallet kommer EXISO AB att vidta åtgärder för att agera enligt EU/US Privacy Shield Agreement.

KONTAKTA OSS

Om du har några som helst funderingar kring hur och varför vi hanterar personuppgifter och cookies är du välkommen att kontakta oss direkt på info@exiso.se

ÄNDRING AV PERSONUPPGIFTSPOLICY

EXISO AB förbehåller sig rätten att ändra denna personuppgiftspolicy vid behov. Om policyn ändras kommer du att informeras om förändringen påverkar behandlingen av dina personuppgifter. Senaste versionen av personuppgiftspolicyn finns alltid tillgänglig på: www.exiso.se. Högst upp på första sidan av denna policy ser du datum för senaste uppdatering

Personuppgiftsincident

En personuppgiftsincident är en säkerhetshändelse där personuppgifter har förstörts, oavsiktligt eller olagligt, röjts till någon obehörig, gått förlorade eller ändrats. När en personuppgiftsincident inträffar måste först sannolikheten och allvaret fastställas, och därefter den följande risken för människors rättigheter och friheter. Om det är troligt att personuppgiftsincidenten kommer att medföra en risk för de registrerade måste Datainspektionen meddelas inom 72 timmar. Om personuppgifts-incidenten är allvarlig så ska även den registrerade utan dröjsmål informeras. Oavsett vilket beslut som fattas så ska det motiveras och dokumenteras.

Vid misstanke om att en personuppgiftsincident har uppstått ska detta omgående rapporteras till administratör som hanterar incidenten enligt föreskrifter.