

Syftet med denna policy för allmän dataskyddsförordning (GDPR) är att fastställa tydliga riktlinjer och procedurer för insamling, behandling och skydd av personuppgifter inom MEXL AB. Denna policy tjänar följande huvudsakliga syften:

Efterlevnad av GDPR: Policyn är utformad för att säkerställa fullständig efterlevnad av bestämmelserna i Europeiska unionens allmänna dataskyddsförordning (GDPR), som syftar till att skydda individers grundläggande rättigheter och friheter i samband med behandling av personuppgifter.

Skydd av registrerades rättigheter: Det är vårt åtagande att skydda integriteten och rättigheterna för registrerade, inklusive våra kunder, anställda och andra individer vars personuppgifter vi behandlar. Vi kommer att säkerställa att deras rättigheter till integritet, transparens och kontroll över deras data respekteras och upprätthålls.

Datasäkerhet: Denna policy beskriver de åtgärder och skyddsåtgärder vi har på plats för att skydda personuppgifter mot obehörig åtkomst, avslöjande, ändring eller förstörelse. Vår organisation är dedikerad till att upprätthålla konfidentialitet, integritet och tillgänglighet av personuppgifter.

Ansvar och ansvarsskyldighet: Vi fastställer roller och ansvar för personal som är involverad i databehandling, från datakontrollanter till databehandlare. Detta säkerställer ansvarsskyldighet och transparens i våra databehandlingsaktiviteter.

Definitioner:

- **Personuppgifter:** Personuppgifter, i samband med dataskydds- och integritetsregler som allmän dataskyddsförordning (GDPR), avser all information som kan användas för att identifiera en individ, antingen direkt eller indirekt. Det omfattar ett brett spektrum av information, och definitionen av personuppgifter är avsiktligt omfattande för att skydda individers integritet.
- **Registrerad:** En levande person som kan identifieras direkt eller indirekt av den information som samlas in och behandlas, antingen ensam eller i kombination med andra data. Personuppgifter kan inkludera ett brett spektrum av information, såsom en persons namn, adress, e-post, telefonnummer, ID-nummer, IP-adress eller annan data som kan användas för att identifiera dem.

- **Datakontrollant:** En person som bestämmer varför och hur personuppgifter ska behandlas. De har huvudansvaret för att säkerställa att databehandlingsaktiviteter utförs i enlighet med dataskyddsregler.
- **Databehandlare:** En anställd på MEXL. AB som behandlar personuppgifter enligt instruktioner och på uppdrag av datakontrollanten.

Denna GDPR-policy gäller för alla aktiviteter inom MEXL. AB som involverar behandling av personuppgifter, oavsett medium, format eller plats för data. Policyns omfattning inkluderar, men är inte begränsad till, följande:

- **Databehandlingsaktiviteter:** Denna policy täcker alla databehandlingsaktiviteter som utförs av MEXL. AB, oavsett om data samlas in från kunder, anställda, leverantörer eller andra intressenter.
- **Datahantering:** Det inkluderar insamling, lagring, hämtning, användning, delning, överföring och bortskaffande av personuppgifter i alla former, inklusive elektronisk, pappersbaserad och muntlig kommunikation.
- **Registrerade:** Policyn gäller personuppgifter för alla registrerade, vilket kan inkludera kunder, anställda, entreprenörer, leverantörer och andra individer vars data vi behandlar.
- **Personal:** Alla anställda, entreprenörer och tredje parter som agerar på uppdrag av MEXL. AB måste följa denna policy i sina databehandlingsaktiviteter.
- **Tredjepartsdatabehandlare:** Denna policy sträcker sig till tredje parts organisationer eller individer som behandlar personuppgifter på uppdrag av vår organisation. Det kräver att de uppfyller samma dataskyddsstandarder som vår organisation.
- **Global räckvidd:** Även om vår organisation är baserad i Sverige har denna policy global räckvidd, eftersom vi kan behandla personuppgifter för individer inom Europeiska unionen (EU) eller andra regioner, underkastade GDPR.

Personuppgifter inkluderar följande:

- **Finansiell information:** Bankkontouppgifter, kreditkortsnummer, finansiell transaktionshistorik.
- **Hälso- och medicinska data:** Medicinska journaler, sjukförsäkringsinformation, genetiska data, biometriska data (t.ex. fingeravtryck, DNA).
- **Anställningsinformation:** Anställningshistorik, lön och förmånsdata, HR-poster.
- **Utbildningsinformation:** Akademiska journaler, student-ID-nummer.

- **Platsdata:** GPS-data, platsövervakningsdata.
- **Bilder och foton:** Fotografier, CCTV-bilder.
- **Sociala medieprofiler:** Användarnamn och profiler på sociala medieplattformar, inlägg, kommentarer och meddelanden.
- **Preferenser och intressen:** Information om en individs preferenser, hobbyer och intressen.
- **Annan information specifik för en individ:** All data som, på egen hand eller i kombination med annan data, kan användas för att identifiera en individ.

Registrerad person har rätt till:

- **Rätt till tillgång:** Rätten att begära och få en kopia av sina personuppgifter som innehas av datakontrollanter.
- **Rätt till rättelse:** Rätten att få felaktigheter i sina personuppgifter korrigerade.
- **Rätt till radering (rätten att bli glömd):** Rätten att begära radering av sina personuppgifter under vissa förhållanden.
- **Rätt att begränsa behandling:** Rätten att begränsa behandlingen av sina data i specifika situationer.
- **Rätt till dataportabilitet:** Rätten att få sina personuppgifter i ett strukturerat, allmänt använt och maskinläsbart format.
- **Rätt att invända:** Rätten att invända mot vissa typer av databehandling, inklusive direktmarknadsföring.
- **Rätt att bli informerad:** Rätten att bli informerad om insamling och användning av sina personuppgifter.
- **Rätt att inte bli föremål för automatiserat beslutsfattande:** Rätten att undvika beslut som enbart baseras på automatiserad behandling som kan ha betydande juridiska eller andra effekter.

Datakontrollanter är ansvariga för flera nyckeluppgifter, inklusive:

- Definiera syftena för vilka personuppgifter ska behandlas.
- Säkerställa att personuppgifter behandlas lagligt, rättvist och transparent.
- Få individers samtycke (när det krävs) eller använda andra rättsliga grunder för databehandling.
- Implementera lämpliga dataskyddspolicyer och åtgärder för att skydda data.
- Uppfylla registrerades begäran om att utöva sina rättigheter, såsom att ge tillgång till deras data eller radera den.
- Rapportera dataintrång till relevanta dataskyddsmyndigheter och, i vissa fall, till berörda individer.

- Genomföra konsekvensbedömningar av dataskydd (DPIAs) när högriskdatabehandlingsaktiviteter planeras.
- Säkerställa att tredje parts databehandlare (om de används) följer dataskyddslagar genom skriftliga avtal och överenskommelser.
- Hålla register över databehandlingsaktiviteter och göra dem tillgängliga för dataskyddsmyndigheter.

Databehandlare är främst ansvariga för att behandla personuppgifter enligt datakontrollantens instruktioner.

- De bör implementera lämpliga säkerhetsåtgärder för att skydda data, rapportera dataintrång till datakontrollanten och hjälpa datakontrollanten att uppfylla registrerades rättighetsbegäran (t.ex. att ge tillgång till, rätta eller radera data).
- Databehandlare måste också hjälpa datakontrollanten att genomföra konsekvensbedömningar av dataskydd (DPIAs) där det är nödvändigt.
- **Underbehandlare:** Databehandlare kan använda underbehandlare för att hjälpa till med att utföra sina databehandlingsaktiviteter. Om en databehandlare engagerar en underbehandlare måste de informera datakontrollanten och säkerställa att underbehandlaren också följer dataskyddsregler.
- **Internationella dataöverföringar:** Databehandlare som är involverade i gränsöverskridande databehandling måste följa regler relaterade till internationella dataöverföringar, såsom att använda standardavtalsklausuler eller andra lagliga mekanismer för att säkerställa skyddet av registrerades rättigheter.
- De bör också vara medvetna om sin roll i att hjälpa datakontrollanter att uppfylla sina GDPR-åtaganden. Detta inkluderar samarbete med revisioner, svara på dataskyddsmyndigheters förfrågningar och säkerställa transparens i databehandlingsaktiviteter.

Allmänna säkerhetsåtgärder

- Databehandlaren ska implementera och upprätthålla lämpliga tekniska och organisatoriska säkerhetsåtgärder för att säkerställa en säkerhetsnivå som är lämplig för risken som är involverad i behandlingen av personuppgifter. Sådana åtgärder ska inkludera, men är inte begränsade till:
- **Data kryptering:** Databehandlaren ska använda krypteringsåtgärder för att skydda personuppgifter under överföring och lagring. Krypteringsmetoder ska vara branschstandard och lämpliga för datans känslighet.

- **Åtkomstkontroll:** Databehandlaren ska säkerställa att åtkomst till personuppgifter är begränsad till auktoriserad personal endast. Åtkomstkontroller, inklusive användarautentisering och rollbaserad åtkomst, ska implementeras.
- **Dataminimering:** Databehandlaren ska endast behandla personuppgifter som är nödvändiga för de definierade syftena. Principer för dataminimering ska tillämpas vid behandling av personuppgifter.
- **Regelbundna säkerhetsrevisioner:** Databehandlaren ska genomföra regelbundna säkerhetsrevisioner och bedömningar för att identifiera och åtgärda sårbarheter och risker för personuppgifter.
- **Utbildning av anställda:** Databehandlaren ska tillhandahålla utbildning till sin personal om dataskydds- och säkerhetsåtgärder, inklusive hantering av personuppgifter.
- Databehandlaren ska dokumentera dessa säkerhetsåtgärder och göra dem tillgängliga för datakontrollanten på begäran.

Respons på dataintrång

- Vid ett personuppgiftsbrott ska databehandlaren omedelbart meddela datakontrollanten om brottet. Databehandlaren ska vidta omedelbara åtgärder för att minska riskerna och återställa datans integritet. Databehandlaren ska också hjälpa datakontrollanten att uppfylla sina skyldigheter att rapportera brottet till relevanta dataskyddsmyndigheter och registrerade.

Revision och efterlevnad

- Databehandlaren ska samarbeta med alla revisioner, inspektioner eller bedömningar relaterade till dataskydd som utförs av datakontrollanten eller relevanta dataskyddsmyndigheter. Databehandlaren ska tillhandahålla all nödvändig information och åtkomst för att underlätta sådana revisioner.