Policy för behandling av personuppgifter

1. Bakgrund

1.1 Mål och syfte

Mål och syfte med denna policy är att säkerställa att Bolaget behandlar personuppgifter lagenligt, säkert och med respekt för den enskildes integritet. Policyn syftar till att beskriva hur personuppgifter ska hanteras inom Bolaget på ett ansvarsfullt och transparent sätt, samt även främja en medveten dataskyddskultur inom Bolaget, i enlighet med Europaparlamentet och Rådets förordning (EU) 2016/679 (Dataskyddsförordningen) (GDPR).

1.3 Tillämpningsområden

Denna policy ska tillämpas inom Outsource i Malmö AB, nedan kallat ”Bolaget”. Bestämmelserna i denna policy omfattar samtliga anställda och uppdragstagare som behandlar personuppgifter under Bolagets ansvar.

1.4 Definitioner

- **personuppgifter:** varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,
- **behandling**: en åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring,
- **personuppgiftsansvarig:** en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt,
- **personuppgiftsbiträde**: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.
- **personuppgiftsincident:** en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats,

2. Roller och ansvar

Nedan beskrivs de roller inom Bolaget som har en central roll i arbetet med att främja ett effektivt integritetsskydd.

- **Styrelse**
  Bolagets styrelse bär det yttersta ansvaret för Bolagets efterlevnad av GDPR och ansvarar för att fastställa principiella ställningstaganden genom denna policy. Styrelsen ska årligen ompröva och fastställa denna policy.
- **Verkställande direktör**
  Verkställande direktör (VD) ansvarar för uppdatering och implementering av denna policy samt att säkerställa att GDPR efterlevs i den löpande förvaltningen. VD ska vid behov upprätta lämpliga instruktioner och rutiner som mer detaljerat beskriver Bolagets hantering inom ramen för Bolagets personuppgiftshantering.
- **Dataskyddsombud**
  Eftersom Bolaget inom ramen för åtgärder mot penningtvätt och finansiering av terrorism behandlar personuppgifter om brott som även inkluderar fysiska personer, samt behandlar känsliga personuppgifter för anställda ska Bolaget ha ett utsett Dataskyddsombud (DSO). Inom ramen för koncernsamarbetet finns ett gemensamt DSO utsett för alla bolag inom Freedom Group.
  DSO ska ha tillräcklig kompetens för att utföra uppdraget, samt ha en oberoende, rådgivande och kontrollerande roll i Bolaget och ska därför inte fatta beslut i frågor som rör efterlevnaden av lämpliga bestämmelser. DSO ska dock delta i alla beslut som rör dataskydd samt vara kontaktperson gentemot registrerade och IMY (Integritetskyddsmyndigheten). Arbetet ska utföras riskbaserat, vilket innebär att insatser och resurser baseras och prioriteras utifrån de personuppgiftsbehandlingar som medför störst risk för de registrerades fri och rättigheter.
- **Anställda**
  Alla anställda inom Bolaget ansvarar för att efterleva denna policy.

3. Allmänna principer för behandling av personuppgifter

All behandling av personuppgifter i Bolaget ska följa nedanstående allmänna principer. Dessa gäller även avtalsparter som behandlar personuppgifter för Bolagets räkning.

3.1 Laglighet, korrekthet och öppenhet

Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Det innebär att Bolaget ska:

- säkerställa att all behandling av personuppgifter sker med laglig grund i enlighet med bestämmelser i GDPR.
- säkerställa att särskilda personuppgifter och uppgifter om brott endast behandlas i enlighet med kraven i GDPR.
- säkerställa att den registrerade blir informerad om personuppgiftsbehandlingen
- säkerställa att personuppgifter behandlas korrekt och på ett sätt som de registrerade rimligen förväntar sig.

3.2 Ändamålsbegränsning

Personuppgifter får endast samlas in för specifika, uttryckliga och berättigade ändamål. Uppgifterna får inte användas för andra, oförenliga syften. Det innebär att personuppgifter inte får behandlas på ett sätt som är oförenligt med de ändamål som anges i behandlingsregistret och kommunicerats till de registrerade.

3.3 Dataminimering

Endast de uppgifter som är nödvändiga för ändamålet får samlas in och behandlas. Behandlingen ska begränsas till det som är relevant och proportionerligt.

3.4 Riktighet

Personuppgifter ska vara korrekta och, om nödvändigt, uppdaterade. Felaktiga eller inaktuella uppgifter ska rättas eller raderas utan dröjsmål.

3.5 Lagringsminimering

Personuppgifter får inte lagras längre än vad som är nödvändigt för ändamålet med behandlingen. Bolaget ska säkerställa att det finns rutiner för radering och gallring av personuppgifter, för såväl digitalt som fysiskt material, inklusive säkerhetskopior.

3.6 Integritet och konfidentialitet

Bolaget ska implementera tillräckliga tekniska och organisatoriska åtgärder för att säkerställa skydd mot obehörig åtkomst, förlust eller skada. Säkerhetsåtgärderna ska upprätthållas under hela tiden som behandlingen av personuppgifter pågår och innefatta alla typer av behandling, såsom lagring och överföring. Säkerhetsåtgärderna ska anpassas utifrån risken med behandlingen, vilket innebär att särskilt strikta säkerhetsåtgärder ska vidtas vid behandling av särskilda kategorier eller på annat sätt integritetskänsliga personuppgifter.

3.7 Ansvarsskyldighet

Bolaget ska kunna påvisa efterlevnad av de grundläggande principerna. För att uppnå detta ska Bolaget säkerställa att samtliga ställningstaganden, riskbedömningar, beslut och annan hantering som rör dataskyddet i Bolaget dokumenteras.

4. Säkerställande av effektivt integritetskyddsarbete

4.1 Behandlingsregister

Bolaget ska föra ett behandlingsregister över samtliga behandlingar av personuppgifter som utförs inom Bolaget. Behandlingsregistret ska även inkludera information om de behandlingar som utförs i egenskap av personuppgiftsbiträde. Behandlingsregistret ska hållas uppdaterat och på begäran av IMY göra registret tillgängligt för myndigheten.

4.2 Den registrerades rättigheter

Bolaget ska säkerställa tillräckliga resurser och rutiner för hantering av registrerades rättigheter avseende:

- rätt till åtkomst
- rätt till rättelse
- rätt till radering (rätten att bli glömd)
- rätt till begränsning av behandling
- rätt till dataportabilitet (rätten att få sina personuppgifter i ett strukturerat, allmänt använt och maskinläsbart format. De kan också begära att uppgifterna överförs till en annan personuppgiftsansvarig, om det är tekniskt möjligt)
- rätt att invända mot behandlingen
- rätten att inte bli föremål för automatiserat beslutsfattande

Bolaget ska hantera begäranden eller förfrågningar från de registrerade inom regelkrävd tidsram. All kommunikation med den registrerade ska ske på ett tydligt och transparent sätt. Bolaget ska vidta åtgärder för att kunna verifiera den registrerades identitet vid begäran om att utöva sina rättigheter, utan att detta hindrar eller försvårar den registrerades möjlighet att utöva sina rättigheter.

4.3 Personuppgiftsincidenter

Bolaget ska ha förmåga att skyndsamt och säkert kunna hantera personuppgiftsincidenter. Det innebär att det ska finnas rutiner och arbetsbeskrivningar där det framgår hur utredning, bedömning, rapportering och dokumentation av personuppgiftsincidenter ska genomföras samt vem i Bolaget som ansvarar för denna hantering.

Bolaget ska säkerställa att personuppgiftsincidenter hanteras inom de tidsramar som anges i GDPR. Samtliga personuppgiftsincidenter för behandling där Bolaget är personuppgiftsansvarig ska riskbedömas. Personuppgiftsincidenter där risk för de registrerade inte kan uteslutas ska rapporteras till IMY och vid hög risk ska de registrerade meddelas tillsammans med en beskrivning av de åtgärder de kan vidta för att minska personuppgiftsincidentens konsekvenser. Om en incident uppstår avseende behandling där Bolaget är personuppgiftsbiträde ska Bolaget skyndsamt informera den personuppgiftsansvarige och tillhandahålla tillräcklig information för att den personuppgiftsansvariga ska kunna fullgöra sina skyldigheter i GDPR.

4.4 Personuppgiftsbiträden

För de fall då annan part hanterar personuppgifter för bolagets räkning som personuppgiftsbiträde ska ett personuppgiftsbiträdesavtal mellan Bolaget och biträdet upprättas. Bolaget ska säkerställa att Personuppgiftsbiträdet ger tillräckliga garantier för att Bolaget ska kunna fullgöra sina skyldigheter i egenskap av personuppgiftsansvarig. För de fall då Bolaget själv är personuppgiftsbiträde ska Bolaget säkerställa att de krav de omfattas av i egenskap av personuppgiftsbiträde även överförs till underbiträden.

4.5 Konsekvensbedömning

Bolaget ska alltid bedöma om en konsekvensbedömning avseende dataskydd (Data Protection Impact Assessment, DPIA) krävs innan en ny behandling av personuppgifter påbörjas. En DPIA är särskilt nödvändig när behandlingen sannolikt medför en hög risk för de registrerades rättigheter och friheter, exempelvis vid användning av ny teknik, omfattande profilering eller behandling av känsliga uppgifter.

Om tidigare behandlingar inte har genomgått en DPIA och det finns risker som inte tidigare analyserats, ska en sådan bedömning genomföras i efterhand för att säkerställa att behandlingen sker i enlighet med gällande lagkrav på dataskydd uppfylls.

Bolaget ska samråda med DSO i frågor som rör konsekvensbedömningar för att säkerställa att processen genomförs korrekt. Om det, trots vidtagna åtgärder, kvarstår en hög risk för de registrerade, ska ett förhandssamråd genomföras med IMY innan behandlingen får påbörjas.

4.6 Tredjelandsöverföring

Bolaget ska säkerställa att överföring av personuppgifter till tredjeland, det vill säga utanför EU/EES, sker i enlighet med kraven i GDPR. Vid tredjelandsöverföringar som inte omfattas av adekvat skyddsnivå ska en giltig överföringsmekanism säkerställas, såsom av EU-kommissionen utfärdade Standardsavtalsklausuler samt en Transfer Impact Assessment

(TIA) genomföras för att säkerställa att överföringen är laglig, inklusive att tillräckliga kompletterande skyddsåtgärder vidtagits.

4.7 Inbyggt dataskydd och dataskydd som standard

Bolaget ska tillämpa principerna om inbyggt dataskydd och dataskydd som standard i all behandling av personuppgifter. Detta innebär att skydd av personuppgifter integreras redan vid utvecklingen av system, processer och tjänster, samt att högsta möjliga skyddsnivå alltid är förinställd. Endast de personuppgifter som är nödvändiga för ändamålet ska behandlas vid framtagandet av nya system, processer eller tjänster, och lämpliga säkerhetsåtgärder ska vidtas för att skydda de registrerades integritet.

4.8 Utbildning av anställda

Samtliga anställda och andra som deltar i Bolagets verksamhet ska, såväl vid nyanställning som löpande, genomgå tillräcklig utbildning avseende kraven i GDPR och Bolagets interna regler avseende personuppgiftsbehandling.

5. Ändringar

Denna policy ska granskas och uppdateras vid behov och fastställas av Bolagets styrelse minst årligen även om inga ändringar gjorts. VD ansvarar för att uppdatera denna policy inför styrelsens fastställelse.