Dataskyddspolicy för Tamros företag i Sverige

1 Allmänna bestämmelser

1.1 Inledning

Tamro har ett gott anseende tack vare våra medarbetares hårda arbete och positiva inställning. Att skydda våra kunders, patienters, leverantörers, affärspartners och medarbetares personuppgifter är av yttersta vikt för Tamro. Brott mot dataskyddslagstiftning kan få allvarliga konsekvenser, såsom böter och officiella utredningar. Den allvarligaste konsekvensen skulle dock vara om vårt anseende skadas. I denna policy beskrivs de åtgärder som Tamros medarbetare ska vidta i syfte att skydda integriteten och konfidentialiteten för de personuppgifter som behandlas inom organisationen, vilket stöds till fullo av Tamros ledning.

1.2 Syfte

I denna policy beskrivs de bestämmelser som gäller vid behandling av personuppgifter för Tamros företag i Sverige i syfte att skydda de registrerade. Syftet med denna policy är att skydda den registrerades grundläggande fri- och rättigheter i enlighet med dataskyddslagstiftningen (inklusive, men inte begränsat till, den europeiska allmänna dataskyddsförordningen (GDPR)).

1.3 Materiellt tillämpningsområde[1]

Denna policy ska tillämpas på sådan behandling av personuppgifter och särskilda personuppgifter som avser fysiska personer som kan identifieras utifrån dessa uppgifter. Den ska tillämpas på uppgifter som behandlas antingen elektroniskt eller som är pappersbaserade och som lagras i ett register.

Denna policy är avsedd att användas tillsammans med Tamros befintliga policyer.

1.4 Territoriellt tillämpningsområde[2]

Denna policy ska tillämpas inom alla organisationer och verksamheter inom Tamro i Sverige.

[1] Art. 2 i dataskyddsförordningen.
[2] Art. 3 i dataskyddsförordningen.

1.5 Lagstiftning

Denna policy bygger på bestämmelserna i den europeiska dataskyddslagstiftningen (särskilt dataskyddsförordningen) som fastställer hårda dataskyddskrav och gäller i alla EU:s medlemsstater.

På vissa områden kan enskilda medlemsstaters nationella lagar och förordningar vara strängare än EU:s. PHOENIX-koncernens samtliga organisationer och medarbetare ska följa tillämplig lokal lagstiftning.

1.6 Ändring av policy

Tamros Ledning förbehåller sig rätten att ändra eller modifiera denna policy i samråd med ansvarigt dataskyddsombud. De anställda på Tamro måste följa bestämmelserna i denna policy.

1.7 Definitioner[3]

I denna policy (och i enlighet med dataskyddsförordningen) avses med

I. *samtycke* av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne,

II. *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,

III. *uppgifter om hälsa*: personuppgifter som rör en fysisk persons fysiska eller psykiska hälsa, inbegripet tillhandahållande av hälso- och sjukvårdstjänster, vilka ger information om dennes hälsostatus,

IV. *medarbetare*: person som är anställd av Tamro eller en annan organisation inom PHOENIX-koncernen,

[3] Art. 4 i dataskyddsförordningen.

V. *register*: en strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden,

VI. *personuppgifter*: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift, en nätidentifierare eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet,

VII. *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,

VIII. *känsliga personuppgifter*: särskilda kategorier av personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning,

IX. *PHOENIX-koncernen:* alla företag i vilka aktiemajoriteten innehas av en organisation inom PHOENIX-koncernen,

X. *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,

XI. *personuppgiftsbiträde*: en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning,

XII. *ansvarigt dataskyddsombud*: organisationens dataskyddsombud, det lokala dataskyddsombudet i ditt land, den lokala dataskyddssamordnaren i ditt land eller koncernens dataskyddschef,

XIII. *begränsning av behandling*: markering av lagrade personuppgifter med syftet att begränsa behandlingen av dessa i framtiden.

2 Principer

2.1 Principer för behandling av personuppgifter[4]

Laglighet, korrekthet och öppenhet[5]

Behandlingen ska ske på ett lagligt, korrekt och öppet sätt. Behandlingen är endast laglig om

a. den registrerade har lämnat sitt samtycke (se avsnitt 2.2 i denna policy)
b. behandlingen är nödvändig för att fullgöra ett avtal
c. behandlingen är nödvändig för att fullgöra en rättslig förpliktelse
d. behandlingen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller för en annan fysisk person
e. behandlingen är nödvändig för att utföra en uppgift av allmänt intresse, **eller**
f. behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen.

Ändamålsbegränsning[6]

Personuppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Kontakta ansvarigt dataskyddsombud i förväg (innan planer införs) om ändamålen med behandlingen ändras.

Uppgiftsminimering

Personuppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Uppgifterna ska raderas om de inte längre behövs. Tamros ledning ska säkerställa att de lokala kraven avseende lagring och radering uppfylls.

Alla medarbetare ska granska sina register regelbundet (minst en gång per år) och om lämpligt radera dem för att uppfylla lokala krav. Avdelningscheferna är ansvariga för dessa granskningar.

---

[4] Art. 5 i dataskyddsförordningen.
[5] Art. 6 i dataskyddsförordningen.
[6] Art. 5 i dataskyddsförordningen.

Alla medarbetare ska informera ansvarigt dataskyddsombud vid oriktigheter avseende raderingsåtgärder och uppgiftstillgångar utan tydliga eller till och med felaktiga regler för radering.

Mer information finns i ”Riktlinjer för lagring av register” (se **bilaga 1**).

Korrekthet

Personuppgifter ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

Lagringsminimering[7]

Personuppgifter får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas.

Integritet och konfidentialitet[8]

Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Ansvarsskyldighet

Tamro ska, som personuppgiftsansvarig, ansvara för och kunna visa att principerna från dataskyddsförordningen som anges ovan efterlevs. Alla medarbetare måste genomgå PHOENIX-koncernens dataskyddsutbildning.

Den personuppgiftsansvarige ska föra ett fullständigt register över behandlingsåtgärder[9]. Alla medarbetare (särskilt avdelningschefer) måste informera ansvarigt dataskyddsombud i förväg (innan planer införs) om ny eller ändrad behandling av personuppgifter så att de kan anpassa registren och kontrollera kraven för behandlingen.

2.2 Villkor för samtycke[10]

Om behandlingen grundar sig på samtycke kan samtycket endast anses vara lagligt om det lämnas genom en entydig bekräftande handling som innebär ett frivilligt, specifikt,

[7] Art. 5 i dataskyddsförordningen.
[8] Art. 5 i dataskyddsförordningen.
[9] Art. 30 i dataskyddsförordningen.
[10] Art. 7 i dataskyddsförordningen.

informerat och otvetydigt medgivande från den registrerades sida om att denne godkänner behandling av personuppgifter som rör honom eller henne.[11] Dessutom måste följande villkor vara uppfyllda:

a) Samtycket ska förvaras i en form som kan användas för att visa att den registrerade har lämnat sitt samtycke till att hans eller hennes personuppgifter behandlas.
b) Begäran om samtycke som lämnas i en skriftlig förklaring som också rör andra frågor ska läggas fram på ett sätt som klart och tydligt kan särskiljas från de andra frågorna i en begriplig och lättillgänglig form, med användning av ett klart och tydligt språk.
c) Den registrerade ska ha rätt att när som helst enkelt återkalla sitt samtycke. Innan samtycke lämnas ska den registrerade informeras om hur samtycket kan återkallas.
d) Samtycke från barn under 13 år avseende informationssamhällets tjänster[12] (t.ex. onlinetjänster) ska endast anses vara lagligt om samtycke ges eller godkänns av den person som har föräldraansvar för barnet.[13]

Kontakta ansvarigt dataskyddsombud för mallar för samtyckesformulär.

2.3 Behandling av särskilda kategorier av personuppgifter[14]

Behandling av särskilda personuppgifter är förbjuden, såvida inte

a. den registrerade uttryckligen har lämnat sitt samtycke
b. behandlingen är nödvändig inom områden som arbetsrätten och social trygghet
c. behandlingen är nödvändig för att skydda den registrerades grundläggande intressen
d. behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk
e. behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade
f. behandlingen är nödvändig för skäl som hör samman med medicinska diagnoser, tillhandahållande av hälso- och sjukvård, social omsorg eller behandling, **eller**
g. behandlingen är nödvändig av skäl av allmänt intresse på folkhälsoområdet. I dessa fall måste dessa uppgifter behandlas av eller under ansvar av en yrkesutövare som omfattas av tystnadsplikt eller av en annan person som också omfattas av tystnadsplikt.

[11] Skäl 32.

[12] Informationssamhällets tjänster avser tjänster som vanligtvis utförs mot ersättning på distans, på elektronisk väg och på individuell begäran av en tjänstemottagare.

[13] Art. 8 i dataskyddsförordningen.

[14] Art. 9 i dataskyddsförordningen.

Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder får endast utföras under kontroll av en offentlig myndighet eller då behandling är tillåten enligt nationell rätt.[15]

3 Den registrerades rättigheter

3.1 Klar och tydlig information och kommunikation samt klara och tydliga villkor för utövandet av den registrerades rättigheter

Samtliga registrerade har följande rättigheter:

- Rätt till tillgång
- Rätt till rättelse
- Rätt till radering
- Rätt till begränsning av behandling
- Rätt till dataportabilitet
- Rätt att göra invändningar

Tamro ska, som personuppgiftsansvarig, vidta nödvändiga åtgärder för att kontrollera identiteten på den registrerade innan denne vidtar åtgärder avseende någon av de rättigheter som anges ovan. All information och kommunikation som avser behandling som lämnas till den registrerade ska vara koncis, klar och tydlig, begriplig och lättillgänglig samt ha ett klart och tydligt språk. Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Den personuppgiftsansvarige ska utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla information.

3.2 Information ska tillhandahållas om personuppgifterna samlas in från den registrerade och om personuppgifterna inte har erhållits från den registrerade[16]

Oavsett om personuppgifterna erhålls direkt från den registrerade eller inte är Tamro skyldig att lämna den information som krävs till den registrerade. Detta ska ske antingen vid insamling eller inom en rimlig period efter det att uppgifterna har erhållits från annan källa. Detta måste dock göras inom en månad. Kontakta din avdelningschef och/eller ansvarigt dataskyddsombud för exempel på informationsmallar.

[15] Art. 10 i dataskyddsförordningen.
[16] Art. 13 och 14 i dataskyddsförordningen.

3.3 Den registrerades rätt till tillgång[17]

Den registrerade ska ha rätt att av Tamro, som personuppgiftsansvarig, få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas. Om så är fallet måste den registrerade vid begäran få tillgång till personuppgifterna och ytterligare information, närmare bestämt ändamålen med behandlingen, de kategorier av personuppgifter som behandlingen gäller etc. Kontakta din avdelningschef och/eller ansvarigt dataskyddsombud för att kontrollera om och hur en sådan begäran om tillgång ska besvaras.

3.4 Rätt till rättelse[18]

Den registrerade har rätt att få felaktiga personuppgifter som rör honom eller henne rättade och att ofullständiga personuppgifter kompletteras (bland annat genom ett kompletterande utlåtande). En sådan begäran ska behandlas utan onödigt dröjsmål.

3.5 Rätt till radering (”rätten att bli bortglömd”)[19]

Den registrerade har rätt att begära att dess personuppgifter raderas, t.ex. om personuppgifterna inte längre är nödvändiga för de ändamål för vilka Tamro ursprungligen samlade in dem, eller om den registrerade återkallar sitt samtycke. Om Tamro, som personuppgiftsansvarig, har offentliggjort personuppgifterna ska de vidta rimliga åtgärder för att underrätta personuppgiftsansvariga som behandlar personuppgifterna om att den registrerade har begärt att personuppgifterna ska raderas (”rätten att bli bortglömd”). Tamro behöver inte ta bort personuppgifterna i samtliga fall, t.ex. om de behöver dem för att fullgöra en rättslig förpliktelse. Kontakta din avdelningschef och/eller ansvarigt dataskyddsombud i dessa fall.

3.6 Rätt till begränsning av behandling[20]

Den registrerade har rätt att kräva att behandlingen av dess personuppgifter begränsas, t.ex. om Tamro, som personuppgiftsansvarig, inte längre behöver personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk. Kontakta din avdelningschef och/eller ansvarigt dataskyddsombud i dessa fall.

---

[17] Art. 15 i dataskyddsförordningen.
[18] Art. 16 i dataskyddsförordningen.
[19] Art. 17 i dataskyddsförordningen.
[20] Art. 18 i dataskyddsförordningen.

Tamro ska, som personuppgiftsansvarig, vidta rimliga åtgärder för att underrätta mottagare till vilka personuppgifterna har lämnats ut om begäran om begränsning.

3.7 Rätt till dataportabilitet[21]

Den registrerade har rätt att få kopior på de personuppgifter som han eller hon har tillhandahållit Tamro, som personuppgiftsansvarig, i ett strukturerat, allmänt använt och maskinläsbart format. Den registrerade har rätt att begära att personuppgifterna överförs från den personuppgiftsansvarige till en annan personuppgiftsansvarig. Detta gäller när behandlingen grundar sig på samtycke eller på ett avtal och behandlingen sker automatiserat. Kontakta din avdelningschef och/eller ansvarigt dataskyddsombud i dessa fall.

3.8 Rätt att göra invändningar[22]

Den registrerade har rätt att när som helst göra invändningar mot behandling av personuppgifter rörande honom eller henne, i synnerhet vid behandling för direkt marknadsföring, profilering och forskningsändamål. Tamro får, som personuppgiftsansvarig, inte längre behandla personuppgifterna såvida inte de inte kan påvisa tvingande berättigade skäl för behandlingen. Kontakta din avdelningschef och/eller ansvarigt dataskyddsombud i dessa fall.

4 Personuppgiftsansvarig och personuppgiftsbiträde

4.1 Säkerhet i samband med behandlingen

Tamro ska, som personuppgiftsansvarig, vidta lämpliga tekniska och organisatoriska åtgärder (dvs. pseudonymisering och kryptering av personuppgifter) för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken[23]. Detta för att fortlöpande säkerställa konfidentialitet, integritet, tillgänglighet och motståndskraft hos behandlingssystemen och -tjänsterna, som beskrivs i PHOENIX-koncernens informationssäkerhetspolicy. Den personuppgiftsansvarige ska också säkerställa inbyggt dataskydd och dataskydd som standard, så att nödvändiga skyddsåtgärder för att genomföra dataskyddsprinciper integreras. Detta kommer att bidra till att säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas.[24] För att säkerställa att

[21] Art. 20 i dataskyddsförordningen.
[22] Art. 21 i dataskyddsförordningen.
[23] Art. 24 i dataskyddsförordningen.
[24] Art. 25 i dataskyddsförordningen.

ledningssystemet för informationssäkerhet ständigt förbättras och för att garantera anpassning till nya tekniska krav har periodiska översyner och revisionsprocesser införts.[25] Affärskontinuitet och katastrofplanering införs för att säkerställa förmågan att återställa tillgängligheten och tillgången till personuppgifter inom rimlig tid vid en fysisk eller teknisk incident.

4.2 Gemensamt personuppgiftsansvariga

Om två eller flera personuppgiftsansvariga (t.ex. Tamro tillsammans med en extern tjänsteleverantör) gemensamt fastställer ändamålen med och medlen för behandlingen av personuppgifter ska de vara gemensamt personuppgiftsansvariga och behöver ett skriftligt avtal. Kontakta ansvarigt dataskyddsombud för mer information.[26]

4.3 Personuppgiftsbiträden[27]

Behandling som genomförs för en personuppgiftsansvarigs räkning (t.ex. av en tjänsteleverantör inom IT eller HR) är endast tillåten om personuppgiftsbiträdet ger tillräckliga garantier om att säkerställa att den registrerades rättigheter skyddas och om ett avtal har slutits. Personuppgiftsbiträdet ska väljas ut noga och regelbundet granskas. Be ansvarigt dataskyddsombud om ett avtal och en revisionsmall.

Detsamma gäller om Tamro behandlar personuppgifter för en annan organisations räkning (t.ex. PHOENIX group IT GmbH för IT-tjänster).

Dessutom måste åtgärder vidtas för att säkerställa att personuppgiftsbiträdet följer de informationssäkerhetsstandarder som anges i PHOENIX-koncernens informationssäkerhetspolicy och endast behandlar personuppgifter enligt instruktionerna.[28] Det är förbjudet att behandla personuppgifter tillhörande en EU-medborgare om behandlingen sker utanför EU, såvida inte de särskilda villkoren avseende överföring av personuppgifter är uppfyllda (se kapitel 5 i denna policy).

[25] Art. 32 i dataskyddsförordningen.
[26] Art. 26 i dataskyddsförordningen.
[27] Art. 28 i dataskyddsförordningen.
[28] Art. 29 i dataskyddsförordningen.

4.4 Samarbete med tillsynsmyndigheten

Tamro och dess medarbetare är skyldiga att samarbeta med Datainspektionen. Om du som anställd kontaktas av Datainspektionen ska du omedelbart kontakta ansvarigt dataskyddsombud.[29]

4.5 Personuppgiftsincident

Alla personuppgiftsincidenter ska omedelbart rapporteras till ansvarigt dataskyddsombud av medarbetaren eller avdelningschefen via PHOENIX-koncernens portal. Om incidenten sannolikt leder till en hög risk för de registrerades fri- och rättigheter ska den registrerade informeras om detta utan onödigt dröjsmål.[30]

Om personuppgiftsincidenten sannolikt leder till en risk för de registrerades fri- och rättigheter ska den lokala tillsynsmyndigheten utan onödigt dröjsmål informeras (av ansvarigt dataskyddsombud). Detta måste göras inom 72 timmar efter att man har fått vetskap om incidenten.[31]

För incidenter som rör hela koncernen ska det lokala dataskyddsombudet eller den lokala dataskyddssamordnaren även informera koncernens dataskyddschef.

För att minska de risker som en personuppgiftsincident medför och för att underlätta rapporteringen till både tillsynsmyndigheterna och de berörda registrerade måste motsvarande process för personuppgiftsincidenter följas vid respektive personuppgiftsincident i syfte att säkerställa att kraven i dataskyddslagstiftningen uppfylls. Mer information finns i ”Riktlinjer för personuppgiftsincidenter” (se **bilaga 2**).

Vid frågor om dataskydd eller om du misstänker att personuppgifter behandlas felaktigt kan du kontakta ansvarigt dataskyddsombud.

4.6 Konsekvensbedömning avseende dataskydd

Konsekvensbedömningar avseende dataskydd[32] krävs före behandling om behandlingen av uppgifter, i synnerhet när ny teknik används, sannolikt leder till en hög risk för de registrerades fri- och rättigheter.

En konsekvensbedömning avseende dataskydd krävs vid:

---

[29] Art. 31 i dataskyddsförordningen.
[30] Art. 34 i dataskyddsförordningen.
[31] Art. 33 i dataskyddsförordningen.
[32] Art. 35 i dataskyddsförordningen.

1) Användning av ny teknik.
2) Automatisk behandling, inbegripet profilering, och på vilken beslut grundar sig som har rättsliga följder för fysiska personer.
3) Behandling i stor omfattning av särskilda kategorier av personuppgifter.
4) Behandling av brottslig verksamhet.
5) Systematisk övervakning av en allmän plats i stor omfattning.
6) Se den lokala tillsynsmyndighetens förteckningar för ytterligare fall.

För att säkerställa att konsekvensbedömningen slutförs innan ny eller ändrad behandling av personuppgifter påbörjas, måste den berörda medarbetaren informera sitt ansvariga dataskyddsombud i förväg (innan planerna införs). Kontakta ansvarigt dataskyddsombud som kan tillhandahålla mallar för konsekvensbedömning avseende dataskydd, vägledning och löpande rådgivning.

Det (lokala) dataskyddsombudet ska samråda med Datainspektionen om en konsekvensbedömning avseende dataskydd visar att behandlingen skulle leda till en hög risk för de registrerades fri- och rättigheter om inte den personuppgiftsansvarige vidtar åtgärder för att minska riskerna.

4.7 Utnämning av dataskyddsombudet[33]

Tamro ska fastställa om ett dataskyddsombud måste utses. För att fastställa detta ska lokal lagstiftning och bestämmelserna i dataskyddsförordningen ses över och beaktas. Dataskyddsförordningen anger att ett dataskyddsombud bör utnämnas om kärnverksamheten består av behandling som kräver regelbunden och systematisk övervakning av de registrerade i stor omfattning eller om kärnverksamheten består av behandling i stor omfattning av särskilda kategorier av uppgifter – det rekommenderas i detaljhandelsländer.

Om Tamro utser mer än ett dataskyddsombud bör Tamro utnämna en av dem till lokalt dataskyddsombud. Om inget dataskyddsombud finns bör en person utnämnas till lokal dataskyddssamordnare. Det lokala dataskyddsombudet och/eller den lokala dataskyddssamordnaren ska rapportera till den lokala ledningen. Organisationernas dataskyddsombud, det lokala dataskyddsombudet och den lokala dataskyddssamordnaren ansvarar för att skydda de registrerades rättigheter inom organisationen/landet och ska samarbeta med varandra och med koncernens dataskyddschef.

PHOENIX-koncernen har utsett en koncernomfattande dataskyddschef som samordnar samarbetet kring alla viktiga frågor som rör dataskydd inom PHOENIX-koncernen,

[33] Art. 38 i dataskyddsförordningen.

tillsammans med det lokala dataskyddsombudet och den lokala dataskyddssamordnaren i de länder där PHOENIX-koncernen är verksam samt koncernens informationssäkerhetschef. Koncernens dataskyddschef rapporterar till PHOENIX-koncernens ledning. Koncernens dataskyddschef ska ha ett nära samarbete med länderna inom PHOENIX-koncernen. Deras uppgift är att övervaka om de koncernövergripande policyerna (denna policy samt detaljerade policyer) följs, i syfte att utveckla och uppdatera dem.

Rollerna som utses ska ha erforderliga yrkesmässiga kvalifikationer och kunskaper om lagstiftning och praxis avseende dataskydd.

PHOENIX-koncernen har utsett en koncernomfattande informationssäkerhetschef som rådgör med PHOENIX-koncernen i alla relevanta säkerhetsfrågor. Koncernens informationssäkerhetschef har till uppgift att utveckla, förbättra och övervaka PHOENIX-koncernens informationssäkerhetsstandarder.

4.8 Dataskyddsombudets ställning[34]

Dataskyddsombuden, de lokala dataskyddsombuden, de lokala dataskyddssamordnarna och koncernens dataskyddschef ska på ett korrekt sätt och i god tid delta i alla frågor, projekt, förändringar eller åtgärder som rör bestämmelserna om skyddet av personuppgifter.

Koncernledningen, de lokala ledningsgrupperna och alla medarbetare ska stödja dataskyddsombuden, de lokala dataskyddsombuden, de lokala dataskyddssamordnarna och koncernens dataskyddschef i utförandet av deras arbetsuppgifter.

Dataskyddsombuden, de lokala dataskyddsombuden, de lokala dataskyddssamordnarna och koncernens dataskyddschef ska ha tillgång till tillräckliga resurser baserat på beskaffenheten på och komplexiteten hos organisationens affärsmodell, inbegripet sådant som ska genomföras inom ramen för ömsesidigt bistånd, samarbete och deltagandet i koncernövergripande dataskyddsfrågor och -projekt.

De ska ha en oberoende och skyddad ställning inom organisationen och ska rapportera till högsta förvaltningsnivå inom relevant organisation inom PHOENIX-koncernen.

De ska fungera som naturlig kontaktpunkt för alla registrerade i frågor som rör behandlingen av deras personuppgifter samt vara kontaktpunkt för tillsynsmyndigheterna.

De ska vara bundna av sekretess och/eller konfidentialitet när det gäller genomförandet av deras uppgifter.

[34] Art. 38 i dataskyddsförordningen.

Kontaktuppgifter till ansvariga dataskyddsombud, lokala dataskyddsombud, lokala dataskyddssamordnare och koncernens dataskyddschef ska publiceras på Tamros intranät, COIN eller liknande.

4.9 Dataskyddsombudets uppgifter[35]

Dataskyddsombuden, de lokala dataskyddsombuden, de lokala dataskyddssamordnarna och koncernens dataskyddschef ska ansvara för att informera och ge råd till den personuppgiftsansvarige och personuppgiftsbiträdet inom organisationen/länderna i PHOENIX-koncernen och medarbetarna i organisationen/länderna.

Tamros ledning ska, som personuppgiftsansvarig, säkerställa att bestämmelserna om dataskydd som beskrivs i lagar, förordningar och koncernövergripande policyer följs. Ledningen ansvarar särskilt för att skydda de registrerades rättigheter.

Dataskyddsombuden, de lokala dataskyddsombuden, de lokala dataskyddssamordnarna och koncernens dataskyddschef ska ansvara för att övervaka efterlevnaden av dataskyddsförordningen, lokala lagar och förordningar avseende dataskydd, denna policy och andra angivna policyer för PHOENIX-koncernen för att skydda de registrerades grundläggande fri- och rättigheter i samband med behandling av personuppgifter.

Koncernens dataskyddschef ska i nära samarbete med de lokala dataskyddsombuden och/eller de lokala dataskyddssamordnarna (t.ex. genom regelbundna telefonkonferenser, möten osv.) upprätta ett gemensamt ramverk som kan fungera som ett stödforum för information och rådgivning till lokala organisationer inom PHOENIX-koncernen (som personuppgiftsansvariga eller personuppgiftsbiträden) avseende dataskyddsbestämmelser.

De lokala dataskyddsombuden och de lokala dataskyddssamordnarna ska övervaka och rapportera bristande efterlevnad och möjliga risker inom Tamros verksamhet till koncernens dataskyddschef. De ska informera om kontroller som genomförs av tillsynsmyndigheter. De lokala dataskyddsombuden och de lokala dataskyddssamordnarna ansvarar för att anordna lämplig utbildning och medvetandehöjande aktiviteter för personuppgiftsansvariga, personuppgiftsbiträden och medarbetare i deras länder. Koncernens dataskyddschef ska tillhandahålla koncernövergripande webbaserad utbildning.

För en bättre översikt, se ansvarsområdena i **behörighetsmatrisen (RACI) i bilaga 1.**

[35] Art. 39 i dataskyddsförordningen.

5 Överföring av personuppgifter

Överföring av personuppgifter inom det land där uppgifterna har samlats in, inom Europeiska unionen (EU) och Europeiska ekonomiska samarbetsområdet (EES) (inklusive behandling i ett tredjeland efter överföring) är i allmänhet tillåtet om behandlingen av uppgifterna också är tillåten enligt dataskyddsförordningen (särskilt i enlighet med kapitel II).

Personuppgifter får endast överföras från ett EU-/EES-land till ett tredjeland (utanför EU/EES) om särskilda villkor är uppfyllda. Kontakta ansvarigt dataskyddsombud i dessa fall. Överföring får ske:

- om Europeiska kommissionen har beslutat att tredjelandet säkerställer en adekvat skyddsnivå (”beslut om adekvat skyddsnivå”, t.ex. Schweiz)[36]
- om den mottagande parten har vidtagit lämpliga skyddsåtgärder (t.ex. bindande företagsbestämmelser, standardiserade dataskyddsbestämmelser som antagits av kommissionen, en godkänd uppförandekod)[37]
- vid domstolsbeslut eller beslut från myndigheter om det grundar sig på en internationell överenskommelse[38]
- om överföringen sker i särskilda situationer (t.ex. uttryckligt samtycke från den registrerade, om överföringen är nödvändig för att fullgöra ett avtal, om överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk, om överföringen är nödvändig för att skydda den registrerades grundläggande intressen)[39]
- om överföringen är nödvändig för ändamål som rör den personuppgiftsansvariges tvingande berättigade intressen och den personuppgiftsansvarige informerar tillsynsmyndigheten[40].

6 Rättsmedel, ansvar och sanktioner

Följande rättsmedel är tillgängliga:

- Den registrerades rätt att lämna in klagomål till en tillsynsmyndighet[41].
- En fysisk eller juridisk persons rätt till ett effektivt rättsmedel mot tillsynsmyndighetens beslut[42].

---

[36] Art. 45 i dataskyddsförordningen.
[37] Art. 46 i dataskyddsförordningen.
[38] Art. 48 i dataskyddsförordningen.
[39] Art. 49 i dataskyddsförordningen.
[40] Art. 49, punkt 1 i dataskyddsförordningen, i slutet.
[41] Art. 77 i dataskyddsförordningen.

- Den registrerades rätt till ett effektivt rättsmedel mot en personuppgiftsansvarig eller ett personuppgiftsbiträde[43].
- Den registrerades rätt att anlita ett organ, en organisation eller en sammanslutning utan vinstsyfte[44].

Överträdelser av bestämmelserna kring dataskydd kan leda till att den registrerade lämnar in skadeståndsanspråk avseende ersättning för materiella eller immateriella skador[45]. Myndigheterna kan påföra administrativa sanktionsavgifter på upp till 10 eller 20 miljoner euro, eller, om det gäller ett företag, på upp till 2 eller 4 % av PHOENIX-koncernens totala globala årsomsättning under föregående budgetår[46]. Enligt svensk lag kan överträdelser leda till åtal[47]. Överträdelser från enskilda medarbetares sida kan leda till påföljder enligt svenska disciplinära åtgärder som är förenliga med svensk arbetsrätt.

7 Behandling i anställningsförhållanden

Enligt svensk lag kan det finnas mer specifika regler i lag eller i kollektivavtal för behandling av anställdas personuppgifter i anställningsförhållanden[48].

8 Slutbestämmelser

Denna policy ska tillämpas från och med den 25 maj 2018.

9 Ledningens godkännande

Lars Schenatz	Peter Blomqvist	Mats Johnsson
Eva Backlund Strid	Johan Mossberg	Mikael Brammesjö
Magnus Peterson	Henrik Schylander	

---

[42] Art. 78 i dataskyddsförordningen.
[43] Art. 79 i dataskyddsförordningen.
[44] Art. 80 i dataskyddsförordningen.
[45] Art. 82 i dataskyddsförordningen.
[46] Art. 83 i dataskyddsförordningen.
[47] Art. 84 i dataskyddsförordningen.
[48] Art. 88 i dataskyddsförordningen.

Bilagor:

1. Riktlinjer för lagring av register

2. Riktlinjer för personuppgiftsincidenter

3. Behörighetsmatris (RACI)