# INTERN POLICY FÖR HANTERING AV PERSONUPPGIFTER

Cardrop Sverige AB
Version 0.1, uppdaterad den 2018-05-24

## 1 INNEHÅLLSFÖRTECKNING

## 1 SYFTE OCH OMFATTNING

Cardrop Sverige AB, org. nr. 556977-6619 (”**Bolaget**”) är enligt lag skyldigt att skydda de personuppgifter som hanteras av Bolaget, och på så sätt skydda enskilda personers integritet. Som ett led i att uppfylla denna skyldighet har Bolaget upprättat denna interna policy för hantering av personuppgifter.

## 2 TILLÄMPLIG LAG OCH TILLSYN

**Tillämplig lag**: Dataskyddsförordningen (även kallad GDPR / General Data Protection Regulation) är en EU-förordning som gäller som lag i Sverige och övriga EU-länder från och med den 25 maj 2018. Det kommer även att finnas vissa kompletterande lagregler i den nya svenska dataskyddslagen och andra lagar avseende personuppgiftsbehandling.

**Tillsynsmyndighet**: Integritetsskyddsmyndigheten (f.d. Datainspektionen) är den svenska tillsynsmyndigheten för personuppgiftsbehandling.

GDPR innehåller strängare regler till skydd för de personer vars personuppgifter behandlas. Vidare ger också GDPR tillsynsmyndigheterna fler befogenheter samt möjligheter att vid vissa fall av överträdelser av GDPR besluta om administrativa sanktionsavgifter på upp till 20 miljoner euro eller 4 % av årsomsättningen, beroende på vilket värde som är högst.

Brister i Bolagets hantering av personuppgifter innebär framförallt en risk för kränkning av enskilda personers integritet, men också att Bolagets varumärke och anseende skadas. För att undvika detta är samtliga anställda skyldiga att följa denna policy vid behandling av personuppgifter.

## 3 ANSVAR, FRÅGOR OCH RAPPORTERING

Bolaget har utsett ett dataskyddsombud. Vid frågor om Bolagets personuppgiftsbehandling, vänligen kontakta dataskyddsombudet (DPO):

*Matteo Beghello*
*Tfn 08-276721 / admin@cardrop.com*

Brister, missförhållanden och s.k. personuppgiftsincidenter (se punkt 17.2) ska rapporteras till dataskyddsombudet.

Dataskyddsombudet rapporterar direkt till VD i alla frågor som avser personuppgiftshantering.

## 4 CENTRALA BEGREPP

Följande begrepp har nedan angiven betydelse:

(a) **Personuppgifter** är i korthet alla uppgifter som kan härledas till en (levande) fysisk person, t.ex. personnummer, namn, epost, adress, IP-nummer, hälsouppgifter, eller en kombination av uppgifter som innebär att en person kan identifieras.

(b) Med ”**behandling**” avses alla åtgärder som vidtas beträffande personuppgifter, t.ex. 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.

(c) **Personuppgifts*ansvarig*** är den som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifterna ifråga. Den personuppgiftsansvarige är den som har det huvudsakliga ansvaret för att personuppgifterna behandlas i enlighet med GDPR.

(d) Ett **personuppgifts*biträde*** är den som behandlar personuppgifter för den personuppgiftsansvariges räkning, t.ex. en leverantör av lönehanteringstjänster.

(e) Den ”**Registrerade**” avser den person vars personuppgifter behandlas av Bolaget.

## 5 REDOVISANDE AV REGELEFTERLEVNAD

Bolaget är enligt lag skyldigt att föra register över den personuppgiftsbehandling som företas i Bolaget. Bolaget har upprättat en registerförteckning i verktyget DP Organizer (”**Registret**”). I Registret ska bland annat relevanta personkategorier, kategorier av personuppgifter, ändamål och laglig grund dokumenteras.

Bolagets interna hanteringspolicys och Register ska kontrolleras minst en gång per kvartal, samt ska uppdateras vid behov. Dataskyddsombudet ansvarar för att policydokument och Register hålls uppdaterade.

Dataskyddsombudet har det övergripande ansvaret för att tillse att de personer inom Bolaget som hanterar personuppgifter har tillräckliga kunskaper om hur personuppgifter ska behandlas inom Bolaget.

## 6 GRUNDLÄGGANDE PRINCIPER

Bolaget ska vid all personuppgiftsbehandling iaktta följande principer.

(a) Uppgifterna ska behandlas på ett **lagligt, korrekt** och **öppet** sätt i förhållande till den Registrerade.

(b) Uppgifterna ska samlas in för särskilda, uttryckligt angivna och berättigade **ändamål** och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.

(c) Uppgifterna ska vara **adekvata, relevanta** och **inte för omfattande** i förhållande till de ändamål för vilka de behandlas.

(d) Uppgifterna ska vara **korrekta** och om **nödvändigt uppdaterade**.

(e) Uppgifterna 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, dvs. uppgifterna måste gallras efter viss tid.

(f) Uppgifterna 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**.

## 7 LAGLIG GRUND

### 7.1 Generellt

All behandling av personuppgifter som utförs av Bolaget ska ha laglig grund. I GDPR anges vad som kan utgöra en laglig grund. De vanligaste lagliga grunderna är:

a) Att behandlingen är nödvändig för att fullgöra ett **avtal med den Registrerade**.

b) Att behandlingen är nödvändig för att fullgöra en **rättslig förpliktelse**, t.ex. att spara vissa uppgifter i enlighet med bokföringslagen eller att rapportera vissa uppgifter till Skatteverket.

c) Att **samtycke** finns från den Registrerade. Observera att det ställs stränga krav på hur ett samtycke är utformat för att det ska vara giltigt. Samtycke bör endast användas om det inte går att utföra behandlingen med stöd av en annan laglig grund.

d) Att behandlingen är tillåten med stöd av en **intresseavvägning**, vilket innebär att Bolaget har ett berättigat intresse av behandlingen, som väger tyngre än den Registrerades integritetsintresse. Exempel på åtgärd som kan utföras med stöd av en intresseavvägning är att upprätta en kontaktlista med namn och kontaktuppgifter till anställdas anhöriga för det fall att den anställda skulle råka ut för en olycka. Arbetsgivarens intresse av att upprätta en sådan kontaktlista anses väga över den anhörigas integritetsintresse.

### 7.2 Känsliga personuppgifter

Så kallade känsliga personuppgifter (eller ”särskilda kategorier av personuppgifter”) får inte behandlas om det inte finns en särskild laglig grund enligt Art 9 i GDPR. Känsliga uppgifter är uppgifter som avslöjar:

(a) ras eller etniskt ursprung,

(b) politiska åsikter,

(c) religiös eller filosofisk övertygelse,

(d) biometriska uppgifter (t.ex. fingeravtryck),

(e) medlemskap i fackförening, eller

(f) personuppgifter som rör hälsa eller sexualliv.

## 8 INFORMATION TILL DEREGISTRERADE

Bolaget är skyldigt att självmant tillhandahålla viss information till de personer vars personuppgifter behandlas, i samband med att dessa samlas in. Informationen ska tillhandahållas i en koncis, klar och tydlig, begriplig och lättillgänglig form, med användning av klart och tydligt språk.

*För att uppfylla informationskravet har Bolaget upprättat en integritetspolicy för varje personkategori vars personuppgifter behandlas som ska kommuniceras till de Registrerade. Rutiner för hur informationsgivningen utförs finns i dokumentet “Rutin för informationsgivning till Cardrops användare och kunder”*

## 9 ÖVERFÖRING AV PERSONUPPGIFTER TILL EXTERNA MOTTAGARE

### 9.1 Generellt

Bolaget kan behöva överföra personuppgifter till externa bolag/organisationer, t.ex. sådana leverantörer som behandlar personuppgifter för Bolagets räkning, och myndigheter som Bolaget måste överföra vissa uppgifter till enligt lag (t.ex. Skatteverket).

En lista över samtliga personuppgiftsbiträden och andra mottagare av personuppgifter ska finnas i Registret för varje personkategori.

### 9.2 Personuppgiftsbiträden

Ett externt bolag som behandlar personuppgifter *för Bolagets räkning* är ett s.k. personuppgiftsbiträde. Exempel på detta kan vara ett externt bolag som t.ex. hanterar Bolagets lönespecifikationer. Bolaget är skyldigt att ingå personuppgiftsbiträdesavtal med samtliga personuppgiftsbiträden. Bolaget har upprättat en mall för personuppgiftsbiträdesavtal.

Före anlitande av ett nytt personuppgiftsbiträde ska Bolaget undersöka huruvida personuppgiftsbiträdet kan garantera att personuppgifterna kommer att behandlas i enlighet med GDPR (bl.a. huruvida personuppgiftsbiträdet vidtar tillräckliga säkerhetsåtgärder) samt inom vilket

geografiskt område personuppgiftsbiträdet kommer att behandla personuppgifterna. Om personuppgifterna kommer att behandlas utanför EU/EES, vänligen se punkt 11 nedan.

### 9.3 Samarbetspartners

Banker, kreditinstitut och försäkringsbolag är[självständigt personuppgiftsansvariga för Bolagets kunders personuppgifter. Detta skall i vart fall klargöras genom avtal med respektive samarbetspartner.

### 9.4 Övriga mottagare

Bolaget behöver inte ingå personuppgiftsbiträdesavtal med eventuella inhyrda konsulter som arbetar direkt under Bolagets ledning, i Bolagets lokaler, i Bolagets egna system etc. Däremot ska dessa personer underteckna ett lämpligt sekretessåtagande.

Inte heller behöver personuppgiftsbiträdesavtal ingås med övriga externa mottagare av uppgifter som själva är personuppgiftsansvariga för sin hantering (dvs. som inte behandlar uppgifterna *för Bolagets räkning*), t.ex. Skatteverket.

## 10 ÖVERFÖRING AV PERSONUPPGIFTER UTANFÖR EU/EES

Det är förbjudet att överföra personuppgifter till länder utanför EU/EES om inte särskilda förutsättningar är uppfyllda. Förbudet gäller överföring både till leverantörer och andra mottagare (t.ex. myndigheter) som behandlar personuppgifter utanför EU/EES. Överföring av personuppgifter utanför EU/EES torde dock främst bli aktuellt i samband med att Bolaget anlitar leverantörer för att utföra vissa tjänster.

Bolagets policy är att i första hand anlita leverantörer som kan garantera att eventuell behandling av personuppgifter för Bolagets räkning sker inom EU/EES.

Om leverantör anlitas som inte kan garantera att personuppgifterna endast behandlas inom EU/EES, ska Bolaget säkerställa att det finns laglig grund för överföringen. Nedan följer exempel på vad som kan utgöra en laglig grund för överföringar till leverantör som behandlar personuppgifter utanför EU/EES.

(a) Leverantören har undertecknat standardavtalsklausuler som har godkänts av EU-kommissionen: ”*Commission Decision C(2010)593 Standard Contractual Clauses (processors)”*, eller sådana standardklausuler som ersätter dessa under GDPR, om sådana utfärdas. (Sådana klausuler ska alltså undertecknas vid sidan om personuppgiftsbiträdesavtalet.)

(b) Leverantören är ett amerikanskt bolag som har anslutit sig till ”Privacy Shield” (Privacy Shield är en uppsättning regler som amerikanska bolag kan ansluta sig till);

(c) Det är nödvändigt att överföra vissa personuppgifter till mottagare utanför EU/EES för att fullgöra ett avtal med den Registrerade, eller för att fullgöra ett avtal med annan part i den Registrerades intresse.

Observera att många molntjänster innebär att personuppgifter flyttas mellan olika servrar, och ibland kan dessa vara placerade utanför EU/EES.

I Registren ska eventuell överföring till länder utanför EU/EES dokumenteras, samt vilka åtgärder som har vidtagits för att säkerställa att överföringen är laglig.

## 11 RIKTLINJER FÖR GALLRING

Personuppgifter får inte sparas under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Det betyder att alla personuppgifter som behandlas av Bolaget måste

gallras, dvs. avidentifieras eller förstöras, när de inte längre behövs eller har blivit ovidkommande i förhållande till ändamålet.

Gallringsskyldigheten omfattar alla personuppgifter som behandlas elektroniskt, dvs. även uppgifter som ligger i t.ex. mejlkorgen. Vidare måste även manuella (fysiska) register gallras ut. Däremot finns det ingen skyldighet att gallra ut uppgifter i fysiskt, osorterat material, t.ex. en osorterad hög med papper på skrivbordet.

(a) Att **avidentifiera** uppgifterna innebär att man avlägsnar alla identifieringsmöjligheter så att de uppgifter som fortsättningsvis behandlas inte längre kan kopplas till en fysisk person, vare sig direkt eller indirekt. Krypterade personuppgifter är inte avidentifierade så länge någon kan göra uppgifterna läsbara och därmed identifiera den person som uppgifterna avser.

(b) Att **förstöra** personuppgifterna innebär att de måste förstöras så att de inte går att återskapa. Det räcker inte att bara lägga informationen i papperskorgen på datorn, utan lagringsmediet måste formateras eller skrivas över så att uppgifterna inte längre går att återskapa.

## 12 REGISTERUTDRAG M.M.

### 12.1 Inledning

Registrerade har vissa rättigheter som Bolaget är skyldigt att tillmötesgå på den Registrerades begäran, t.ex. begäran om registerutdrag och rättelse av personuppgifter.

### 12.2 Fastställ identiteten på den som framställer begäran - autentisering

Bolaget måste alltid verifiera identiteten hos den person som framställer en begäran från Bolaget. Detta är av vikt för att inte någon annan än den Registrerade ska kunna fatta beslut om hur dennes uppgifter ska behandlas eller för att någon annan ska få tillgång till den Registrerades uppgifter.

För att säkerställa identiteten hos den Registrerade ska Bolaget tillämpa lämpligt autentiseringsförfarande. Vilken typ av autentiseringsförfarande som ska användas beror framförallt på uppgifternas känslighet och på vilket sätt uppgifterna lämnas ut.

I de fall personuppgifterna som behandlas är att betraka som känsliga, eller dess destruering eller missbruk kan leda till personlig skada för individen, skall alltid personens identitet stärkas genom t ex BankID eller annan godtagbar identifikation likt id-handling eller kontrollfrågor.

### 12.3 Hur snabbt ska Bolaget svara på en begäran?

Bolaget är skyldigt att besvara en begäran enligt nedan utan dröjsmål, och absolut senast inom en månad efter att begäran gjordes.

Bolaget ska eftersträva att i så stor utsträckning som möjligt besvara begäran om registerutdrag och dataportabilitet omedelbart genom att ge fjärråtkomst till ett säkert system genom vilket den Registrerade kan få direkt åtkomst till sina personuppgifter.

Om den Registrerades begäran är komplicerad kan perioden förlängas med max två månader. Om begäran anses vara komplicerad ska dataskyddsombudet rådfrågas.

### 12.4 I vilket format ska Bolaget besvara en begäran?

Om den Registrerade lämnar begäran i elektronisk form, ska begäran besvaras i ett elektroniskt format som är allmänt använt (om den Registrerade inte begär något annat).

Om den Registrerade lämnar begäran brevledes, kan begäran besvaras brevledes.

### 12.5 Får Bolaget ta ut en avgift för att tillmötesgå begäran?

Nej, som regel ska Bolaget besvara begäran kostnadsfritt.

Undantag kan göras om en begäran är uppenbart ogrundad eller orimlig, särskilt på grund av dess repetitiva art. I sådana fall får Bolaget ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillmötesgå begäran, eller vägra att tillmötesgå begäran.

### 12.6 Den Registrerades rättigheter

#### *12.6.1 Registerutdrag*

Bolaget ska på den Registrerades begäran bekräfta huruvida personuppgifter som rör honom eller henne behandlas. Registerutdrag erhålles, efter det att skriftlig handling skickats till Cardrops kundtjänst.

De uppgifter som ska inkluderas i ett registerutdrag är:

a) Ändamålen med behandlingen.

b) De kategorier av personuppgifter som behandlingen gäller.

c) De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer.

d) Om möjligt, den förutsedda period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

e) Förekomsten av rätten att av Bolaget begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den Registrerade eller att invända mot sådan behandling.

f) Rätten att inge klagomål till en tillsynsmyndighet.

g) Om personuppgifterna inte samlas in från den Registrerade, all tillgänglig information om varifrån dessa uppgifter kommer.

h) Förekomsten av automatiserat beslutsfattande, inbegripet profilering, varvid det åtminstone i dessa fall ska lämnas meningsfull information om logiken bakom samt betydelsen och de förutsedda följderna av sådan behandling för den Registrerade.

i) Om personuppgifterna överförs till ett tredjeland eller till en internationell organisation, ska den Registrerade ha rätt till information om de lämpliga skyddsåtgärder som har vidtagits vid överföringen.

**Om ett registerutdrag innehåller personuppgifter om andra personer än den som framställt begäran, ska sådana personuppgifter i regel raderas. Bolaget ska inte heller lämna ut information avseende affärshemligheter, immateriella rättigheter eller liknande information.**

#### *12.6.2 Dataportabilitet*

Rätten till dataportabilitet gäller vid sidan av rätten till registerutdrag. Rätten till dataportabilitet innebär att de Registrerade har rätt att få tillgång till vissa personuppgifter i ett ”strukturerat, allmänt använt och maskinläsbart format”, samt att den Registrerade har rätt att överföra personuppgifterna från en personuppgiftsansvarig till en annan personuppgiftsansvarig.

Export av s k portabel data sker efter det att personens identitet kunnat säkerställas efter det att skriftlig handling skickats till Cardrops kundtjänst. Datan vilken exporteras erbjuds via standarden JSON.

Till skillnad från rätten till registerutdrag gäller rätten till dataportabilitet endast när personuppgiftsbehandlingen grundas på den Registrerades (i) samtycke eller på (ii) ett avtal där den Registrerade är part. Vidare krävs att behandlingen är automatiserad. Dessa förutsättningar får anses vara uppfyllda för viss behandling avseende anställda, konsumenter och företagskunder som är enskilda firmor. Behandling som utförs med stöd av en intresseavvägning omfattas inte av dataportabilitetskravet, t.ex. behandling av anställdas anhörigas personuppgifter eller behandling av kontaktpersoner hos kundföretag som inte är enskilda firmor.

De uppgifter som ska tillhandahållas är samtliga uppgifter som den Registrerade har tillhandahållit Bolaget. Detta innefattar

(i) uppgifter som tillhandahållits genom en aktiv handling (t.ex. när man skapar ett användarkonto), och
(ii) uppgifter som samlats in genom den Registrerades användning av en tjänst, exempelvis den Registrerades sökhistorik på en webbsida.

Däremot behöver Bolaget inte lämna ut analyser som Bolaget har gjort baserat på den Registrerades uppgifter.

### *12.6.3 Rättelse*

Bolaget ska på den Registrerades begäran rätta felaktiga personuppgifter som rör den Registrerade, samt komplettera ofullständiga personuppgifter baserat på den Registrerades eventuella kompletterande utlåtande.

Rättelse sker efter det att personens identitet kunnat säkerställas. Ansökan om att utföra detta sker antingen via efter det att skriftlig handling skickats till Cardrops kundtjänst.

### *12.6.4 Radering - ”rätten att bli bortglömd”*

Radering av personuppgifter och data sker endast efter det att personens identitet kunnat säkerställas. Ansökan om att utföra detta sker efter det att skriftlig handling skickats till Cardrops kundtjänst.

Den Registrerade har rätt att få sina personuppgifter raderade i följande fall:

(a) Personuppgifterna är **inte längre nödvändiga** för de ändamål för vilka de samlats in eller på annat sätt behandlats.

(b) Den Registrerade **återkallar det samtycke** på vilket behandlingen grundar sig, och det inte finns någon annan rättslig grund för behandlingen.

(c) Den Registrerade invänder mot behandling som grundar sig på en **intresseavvägning**, och det saknas tvingande berättigade skäl för behandlingen som väger tyngre än den Registrerades integritetsintresse.

(d) Den Registrerade invänder mot behandling av dess personuppgifter för **direktmarknadsföring**.

(e) Personuppgifterna har behandlats på **olagligt** sätt.

(f) Personuppgifterna måste raderas för att uppfylla en **rättslig förpliktelse** enligt tillämplig lag som Bolaget omfattas av.

(g) I vissa fall avseende barns personuppgifter.

**Undantag:** Det finns vissa undantag till rätten till radering. Undantag gäller om behandlingen är nödvändig av olika skäl. För Bolaget torde de mest relevanta undantagen vara om behandlingen är nödvändig för att Bolaget ska kunna (i) uppfylla en rättslig förpliktelse som kräver behandling enligt tillämplig lag, eller (ii) för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

### *12.6.5 Begränsning*

Begränsning i hanteringen av personuppgifter och data sker endast efter det att personens identitet kunnat säkerställas. Ansökan om att utföra detta sker efter det att skriftlig handling skickats till Cardrops kundtjänst..

Den Registrerade har rätt att kräva att behandlingen av dennes personuppgifter begränsas i vissa fall, t.ex. om den Registrerade bestrider personuppgifternas korrekthet, under en tid som ger Bolaget möjlighet att kontrollera om personuppgifterna är korrekta, eller om behandlingen är olaglig och den Registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.

### *12.6.6 Anmälningsskyldighet*

Bolaget ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser eller radering av personuppgifter eller begränsningar av behandling som skett, om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Detta innebär att Bolaget i regel ska underrätta sina personuppgiftsbiträden om att en Registrerads personuppgifter har rättats eller raderats.

**Exempel**: Om en anställd byter adress och begär att detta justeras i Bolagets register över anställda, ska Bolaget även underrätta eventuella personuppgiftsbiträden som behandlar anställdas uppgifter, t.ex. den leverantör som hanterar lönespecifikationer.

### *12.6.7 Invändningar, bl.a. mot direktmarknadsföring*

Individen kan alltid genom att kontakta kundtjänst, avsäga sig marknadsföring från Cardrop.

Den Registrerade har, under vissa förutsättningar, rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne.

Denna rätt gäller bl.a. om behandlingen grundar sig på en intresseavvägning. Gör den Registrerade en invändning mot behandling som baseras på en intresseavvägning har Bolaget inte längre rätt att behandla personuppgifterna såvida inte Bolaget kan påvisa (i) tvingande berättigade skäl för behandlingen som väger tyngre än den Registrerades intressen, rättigheter och friheter, eller (ii) om behandlingen sker för fastställande, utövande eller försvar av rättsliga anspråk.

Gör den Registrerade en invändning mot behandling av personuppgifter för direktmarknadsföring har Bolaget inte längre rätt att behandla personuppgifterna för direktmarknadsföring, samt profilering som hänger ihop med detta. Bolaget ska omgående upphöra med all direktmarknadsföring gentemot Registrerade som har motsatt sig detta.

### *12.6.8 Profilering*

Den Registrerade har rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling, inbegripet profilering, vilket har rättsliga följder för honom eller henne eller på liknande sätt i betydande grad påverkar honom eller henne.

## 13 DATASKYDDSOMBUD

Dataskyddsombudet har följande uppgifter:

a) Att informera och ge råd till Bolaget och de anställda som behandlar personuppgifter om deras skyldigheter enligt GDPR och annan tillämplig lag.

b) Att övervaka efterlevnaden av GDPR och annan tillämplig lag, av denna policy och Bolagets övriga policys för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.

c) Om Bolaget ska genomföra en s.k. konsekvensbedömning, ska Dataskyddsombudet ge råd avseende dataskydd och övervaka genomförandet av konsekvensbedömningen.

d) Att samarbeta med tillsynsmyndigheten.

e) Att fungera som kontaktpunkt för tillsynsmyndigheten i frågor som rör behandling, inbegripet eventuella förhandssamråd, och vid behov samråda i alla andra frågor kring databasskydd.

## 14 INBYGGT DATASKYDD

I GDPR finns ett krav på ”inbyggt dataskydd och dataskydd som standard” (även känt under begreppen ”privacy by design” och ”privacy by default”). Bolaget ska arbeta mot att system och processer i största möjliga mån utformas för att uppfylla kraven på inbyggt dataskydd. Detta innebär att Bolaget ska vidta lämpliga tekniska och organisatoriska åtgärder, och att Bolaget ska eftersträva att IT-systemen automatiskt ska leda användaren mot ett integritetssäkert arbetssätt, exempelvis genom att tillämpa grundinställningar som innebär att bara information som behövs samlas in och visas. Vid upphandling av IT-tjänster ska tydliga krav formuleras till eventuella leverantörer av IT-stöd, och dataskyddsfrågorna bör beaktas redan under förstudie och vid kravspecifikation.

## 15 KONSEKVENSBEDÖMNING

Innan en behandling av personuppgifter inleds som kan leda till en hög risk för integritetsintrång, ska Bolaget bedöma konsekvenserna för de Registrerade genom en s.k. konsekvensbedömning. Om man bedömer att behandlingen skulle leda till en hög risk om inte Bolaget vidtar åtgärder för att minska risken, måste man dessutom samråda med Integritetsskyddsmyndigheten genom ett s.k. förhandssamråd.

## 16 IT-SÄKERHET

### 16.1 Generellt

Det åligger Bolaget att vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken. En analys av nuläge finns dokumenterad i s k Data Protection Impact Assesment (DPIA) vilket uppdateras vid behov och genomlyses en gång per kvartal

### 16.2 Personuppgiftsincidenter

#### *16.2.1 Skyldighet att anmäla personuppgiftsincidenter*

Bolaget är skyldigt att anmäla s.k. ”personuppgiftsincidenter” till Integritetsskyddsmyndigheten.

En personuppgiftsincident definieras som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas och även obehörigt röjande av eller obehörig åtkomst till personuppgifterna.

**Samtliga personuppgiftsincidenter som upptäcks av anställda inom Bolaget ska omedelbart rapporteras till dataskyddsombudet och VD.**

När en personuppgiftsincident inträffar har Bolaget en skyldighet att **snarast och senast inom 72 timmar** från upptäckten av incidenten, göra en anmälan till Integritetsskyddsmyndigheten. Skulle det inte vara möjligt att hinna göra anmälan inom 72 timmar, måste anmälan följas av en motivering till förseningen. Är det osannolikt att incidenten leder till några risker för de Registrerades fri- och rättigheter behöver dock inte någon anmälan göras. För att avgöra om en anmälan ska göras eller inte ska Bolaget analysera om incidenten sannolikt kan leda till:

(a) Att de Registrerade förlorar kontroll över sina insamlade personuppgifter.

(b) Att de Registrerades rättigheter inskränks.

(c) Diskriminering, identitetsstöld, bedrägeri, finansiell förlust, skadlig ryktesspridning.

(d) Brott mot sekretess eller tystnadsplikt.

Ett personuppgiftsbiträde har en skyldighet att underrätta Bolaget utan onödigt dröjsmål efter att ha fått vetskap om en personuppgiftsincident. Detta innebär att Bolagets personuppgiftsbiträden är skyldiga att rapportera eventuella incidenter till Bolaget.

### *16.2.2 Vad ska en anmälan innehålla?*

Anmälan till Integritetsskyddsmyndigheten ska innehålla följande information:

(a) En beskrivning av incidenten i fråga.

(b) Vilka kategorier av Registrerade och hur många Registrerade som kan komma att beröras.

(c) Ungefär hur många personuppgifter det rör sig om.

(d) Vilka sannolika konsekvenser incidenten kan få.

(e) Vilka åtgärder som har vidtagits eller föreslagits för att motverka potentiella negativa konsekvenser.

(f) Namn och kontaktuppgifter till dataskyddsombud eller GDPR-ansvarig.

Om inte all information enligt ovan kan lämnas samtidigt får information lämnas i omgångar, dock utan ytterligare dröjsmål. För att Integritetsskyddsmyndigheten ska kunna utföra tillsyn är det även mycket viktigt att alla personuppgiftsincidenter dokumenteras, inklusive orsak, effekter och åtgärder.

Vidare ska Registrerade i vissa fall utan onödigt dröjsmål informeras om personuppgiftsincidenter som medför en anmälningsskyldighet. Information ska innehålla en tydlig och klar beskrivning av personuppgiftsincidenten, sannolika konsekvenser av incidenten, vidtagna eller föreslagna åtgärder samt kontaktuppgifter. Information till Registrerade behöver dock inte lämnas för det fall att något av följande villkor är uppfyllt:

(a) Lämpliga tekniska och organisatoriska skyddsåtgärder avseende de personuppgifter som påverkats av incidenten har vidtagits (särskilt kryptering).

(b) Ytterligare åtgärder har vidtagits som säkerställer att den höga risken enligt ovan sannolikt inte längre kommer att uppstå.

(c) Om det skulle innebära en oproportionell ansträngning att informera de Registrerade kan istället allmänheten informeras eller annan åtgärd vidtas som innebär att informationen når de Registrerade på ett lika effektivt sätt.