RIKTLINJER FÖR S:T ERIK FÖRSÄKRINGS AB:s HANTERING AV PERSONUPPGIFTER

FASTSTÄLLD AV STYRELSEN 2018-05-29

1 Allmänt

Denna instruktion har upprättats mot bakgrund av de regler om behandling av personuppgifter som anges i Förordning (EU) 2016/679, Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning samt DIFS 2018:2.

Riktlinjerna revideras löpande och skall fastställas minst årligen av styrelsen.

Syftet med instruktionen är att klargöra vilka regler som gäller för bolagets hantering av personuppgifter och uppnå laglighet, korrekthet, öppenhet, ändamålsbegränsning, uppgiftsminimering, lagringsminimering integritet och konfidentialitet vid bolaget hantering av personuppgifter och därmed uppfylla bolagets ansvarsskyldighet.

2 Ansvar

2.1 Bolaget (Personuppgiftsansvarig)

Bolaget är personuppgiftsansvarig för sin egen behandling och kan vara gemensamt ansvarig om bolaget och annat subjekt tillsammans fastställer ändamålen med och metoderna för behandlingen.

I de fall bolaget handhar uppgifter för annat subjekts räkning är bolaget personuppgiftsbiträde.

Med beaktande av behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige genomföra lämpliga tekniska och organisatoriska åtgärder för att säkerställa och kunna visa att behandlingen utförs i enlighet med gällande rätt. Dessa åtgärder ska ses över och uppdateras vid behov.

Vidare ansvarar personuppgiftsansvarig för vad som stadgas nedan 2.2.3 avseende dataskyddsombudets oberoende och resurser.

VD har att, inom ramen för förvaltningsåtgärder, tillse att personuppgifter hanteras korrekt av bolaget och kan därvid delegera uppgifter internt och externt.

2.2 Dataskyddsombud

Bolaget hanterar en stor mängd personuppgifter i sin skadehantering och vid uppfyllande av försäkringsavtal. Dessa uppgifter hör till viss del till särskilda kategorier (känsliga) av personuppgifter. Av den anledningen ska bolaget utse ett dataskyddsombud.

2.2.1 Kompetens

Dataskyddsombudet ska utses på grundval av yrkesmässiga kvalifikationer och, i synnerhet, sakkunskap om lagstiftning och praxis avseende dataskydd samt förmågan att fullgöra de uppgifter som avses i Artikel 39.

2.2.2 Uppgifter

Ombudets roll är att kontrollera att dataskyddsförordningen följs inom organisationen genom att till exempel utföra kontroller och informationsinsatser. Dataskyddsombudet ska även vara en kontaktpunkt för tillsynsmyndigheten och de registrerade.

Dataskyddsombudet ska vid utförandet av sina uppgifter ta vederbörlig hänsyn till de risker som är förknippade med behandling, med beaktande av behandlingens art, omfattning, sammanhang och syften.

Dataskyddsombudet ska:

- Informera, utbilda och ge råd till den personuppgiftsansvarige eller personuppgiftsbiträdet och de anställda som behandlar personuppgifter om deras skyldigheter enligt gällande regelverk.

- Övervaka bolagets, anställdas och personuppgiftsbiträdens efterlevnad av gällande rätt, ansvarstilldelning och utbildning.

- Övervaka personuppgiftsansvariges eller personuppgiftsbiträdets strategi för skydd av personuppgifter, inbegripet ansvarstilldelning, information till och utbildning av personal som deltar i behandling och tillhörande granskning.

- På begäran ge råd vad gäller konsekvensbedömningen avseende dataskydd och övervaka genomförandet av den.

- Samarbeta med tillsynsmyndigheten och utgöra kontaktpunkt i frågor som rör behandling, inbegripet förhandssamråd, och vid behov samråda i alla andra frågor.

- Tillse att det finns en registerförteckning.

- Tillse att det finns en mall för personuppgiftsbiträdesavtal.

- Rapportera till styrelsen enligt p 13.

2.2.3 Oberoende

- Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet på ett korrekt sätt och i god tid deltar i alla frågor som rör skyddet av personuppgifter.

- Den personuppgiftsansvarige och personuppgiftsbiträdet ska stödja dataskyddsombudet i utförandet av dennes uppgifter genom att tillhandahålla de resurser som krävs för att fullgöra dessa uppgifter samt tillgång till personuppgifter och behandlingsförfaranden, samt i upprätthållandet av dennes sakkunskap.

- Den personuppgiftsansvarige och personuppgiftsbiträdet ska säkerställa att dataskyddsombudet inte tar emot instruktioner som gäller utförandet av dessa uppgifter. Han eller hon får inte avsättas eller bli föremål för sanktioner av den personuppgiftsansvarige eller personuppgiftsbiträdet för att ha utfört sina uppgifter.

- Dataskyddsombudet ska rapportera direkt till den personuppgiftsansvariges eller personuppgiftsbiträdets högsta förvaltningsnivå.

- Den registrerade får kontakta dataskyddsombudet med avseende på alla frågor som rör behandlingen av dennes personuppgifter och utövandet av dennes rättigheter enligt denna förordning.

- Dataskyddsombudet ska, när det gäller dennes genomförande av sina uppgifter, vara bundet av sekretess eller konfidentialitet i enlighet med unionsrätten eller medlemsstaternas nationella rätt.

- Dataskyddsombudet får fullgöra andra uppgifter och uppdrag. Den personuppgiftsansvarige eller personuppgiftsbiträdet ska se till att sådana uppgifter och uppdrag inte leder till en intressekonflikt. Bolaget har riktlinjer för intressekonflikter som därvid ska följas.

Rättsinformation:
- *Artikel 37-39*
- *Skäl 97*
- *Artikel 29-gruppen, Riktlinjer om dataskyddsombud*

2.2.4 Tystnadsplikt
Dataskyddsombudet får inte obehörigen röja det som ombudet har fått kännedom om vid fullgörandet av sin uppgift.

I det allmännas verksamhet tillämpas offentlighet- och sekretesslagen i stället för första stycket. Sekretess gäller om det kan antas att uppgiften efter utlämnande kommer att behandlas i strid med Dataskyddsförordningen eller Lag med kompletterande bestämmelser till EU:s dataskyddsförordning.

Rättsinformation:
- *Lag (2018:218) med komplettering till EU:s dataskyddsförordning 1 kap. §§ 7-8§.*
- *Offentlighet- och sekretesslagen (2009:400) 10 kap. 27§ samt 21 kap. 7§.*

2.3 Anställda
Anställda ansvarar för att deras behandling av personuppgifter följer gällande rätt och dessa riktlinjer och ska bl.a.:

- Ansvara för att dataskyddsfrågorna beaktas i de system, upphandlingar eller avtal som den anställde ansvarar för.

- Endast behandla personuppgifter om detta är nödvändigt för ett lagligt ändamål, är säkert och då minimera dessa uppgifter.

- Att registrerad fått den information som krävs enligt gällande rätt.

- Upprätta dokument (om sådant inte redan finns upprättat för behandlingen) avseende behandlingen för att utreda och dokumentera om behandlingen kan ske, om konsekvensbedömning är aktuellt samt meddela dataskyddsombudet detta.

- Upprätta personbiträdesavtal inom sitt ansvarsområde.

- Informera dataskyddsombudet i god tid om sådant som kan beröra behandling, ex:
    - Ny eller ändrad behandling
    - Ändringar av de personuppgifter som behandlas
    - Ändringar i IT-system som påverkar personuppgifterna, ex. avseende säkerhet, loggning, backupper, möjligheter till utsökning av information, m.m.
    - Inför upphandling av IT-system eller ändringar av avtal

- Vid behov fråga dataskyddsombudet om råd, särskilt vid konsekvensbedömning.

2.4 Personuppgiftsbiträde

Personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning och som således finns utanför den personuppgiftsansvariges organisation.

Personuppgiftsbiträdet tillgodoser någon annans intressen, måste följa instruktioner och kan således inte bestämma ändamålet med behandlingen.

2.4.1 Anlitande eller antagande av uppdrag som personuppgiftsbiträde/underbiträde

Om bolaget anlitar ett personuppgiftsbiträde eller själv utgör biträde åt annan personuppgifts-ansvarig ska uppdraget hanteras som följer.

- Personuppgiftsbiträde får endast anlitas, eller bolaget anta sådant uppdrag, om biträdet kan garantera lämpliga tekniska och organisatoriska åtgärder på sådant sätt att behandlingen uppfyller gällande rätt och säkerställer att den registrerades rättigheter skyddas.

- Personuppgiftsbiträdet får inte anlita ett annat personuppgiftsbiträde utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits av den personuppgifts-ansvarige.

  Om ett allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet informera den personuppgiftsansvarige om eventuella planer på att anlita nya personuppgifts-biträden eller ersätta personuppgiftsbiträden, så att den personuppgiftsansvarige har möjlighet att göra invändningar mot sådana förändringar.

  I de fall där ett personuppgiftsbiträde anlitar ett underbiträde ska denne genom avtal, åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet eller mellan den personuppgiftsansvarige och personuppgiftsbiträdet och ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller gällande rätt.

  Om det andra underbiträdet inte fullgör sina skyldigheter i fråga om dataskydd ska det ursprungliga personuppgiftsbiträdet vara fullt ansvarig gentemot den personuppgiftsansvarige för utförandet av underbiträdets skyldigheter.

- Personuppgiftsbiträdet ska föra en registerförteckning över sin behandling.

- Skriftligt avtal ska upprättas enligt nedan såvida inte gällande rätt stadgar annat.

2.4.2 Personuppgiftbiträdesavtal

Ett personuppgiftsbiträdesavtal ska vara skriftligt, eller utgöra en del av annat skriftligt avtal, och reglera att:

- föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter anges.

- biträdet endast får behandla personuppgifter på dokumenterade instruktioner från den personuppgiftsansvarige, inbegripet när det gäller överföringar av personuppgifter till ett tredjeland eller en internationell organisation, såvida inte denna behandling krävs enligt unionsrätten eller enligt en medlemsstats nationella rätt som personuppgifts-biträdet omfattas av, och i så fall ska personuppgiftsbiträdet informera den personuppgiftsansvarige om det rättsliga kravet innan uppgifterna behandlas, såvida sådan information inte är förbjuden med hänvisning till ett viktigt allmänintresse enligt denna rätt.

- biträdet säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt.

- biträdet vidtar alla säkerhetsåtgärder enligt nedan.

- biträdet ska respektera de villkor som stadgas i 2.4.1 för anlitandet av ett annat personuppgiftsbiträde (underbiträde)

- biträdet med tanke på behandlingens art, ska hjälpa den personuppgiftsansvarige genom lämpliga tekniska och organisatoriska åtgärder, i den mån detta är möjligt, så att den personuppgiftsansvarige kan fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter.

- biträdet ska bistå den personuppgiftsansvarige med att se till att säkerhet i samband med behandlingen, hantering av personuppgiftsincidenter, konsekvensbedömning av dataskydd och förhandssamråd med tillsynsmyndigheten kan ske (med beaktande av typen av behandling och den information som personuppgiftsbiträdet har att tillgå).

- biträdet beroende på vad den personuppgiftsansvarige väljer, ska radera eller återlämna alla personuppgifter till den personuppgiftsansvarige efter det att tillhandahållandet av behandlingstjänster har avslutats, och radera befintliga kopior såvida inte lagring av personuppgifterna krävs enligt unionsrätten eller medlemsstaternas nationella rätt.

- biträdet ska ge den personuppgiftsansvarige tillgång till all information som krävs för att visa att de skyldigheter som avser personuppgiftsbiträden och anlitande av dessa har fullgjorts samt möjliggöra och bidra till granskningar, inbegripet inspektioner, som genomförs av den personuppgiftsansvarige eller av en annan revisor som bemyndigats av den personuppgiftsansvarige.

Rättsinformation:

- *Artikel 4.8, 28-29*
- *Skäl 81*

3 Process

Behandling av personuppgifter sker på olika nivåer och i olika syften. Det är i den första linjen, verksamheten, som den faktiska behandlingen sker och även där som laglighet och kontroller sker.

Dataskyddsombudet har en övervakande, rådgivande och kontrollerande roll i andra linjen.

Varje typ av ny behandling utreds av den aktuella handläggaren och en till person hos den personuppgiftsansvarige. Utredningen dokumenteras, registerförteckningen uppdateras och information lämnas till dataskyddsombudet (vid konsekvensbedömning ska dataskyddsombudet rådfrågas). Detta innebär att bolagets register byggs upp succesivt och att de behandlingstyper som bolaget har finns dokumenterade.

När samma typ av behandling ska utföras finns således en genomförd kontroll och handläggaren behöver då inte genomföra en utredning igen, såvida inget har ändrats avseende uppgifter och ändamål. Detta ska i sådana fall hanteras som en ny behandling.

Vid upphandling (outsourcing) tillser den som ansvarar för upphandlingen att krav ställs på uppdragstagaren att redovisa sin process för personuppgiftshantering inklusive dataskydd samt att det upprättas personuppgiftsbiträdesavtal som en del av förfrågningsunderlaget. Vidare svarar den ansvariga som en del av sin kontraktsuppföljning att kontroll sker av biträdet. Dataskyddsombudet övervakar att krav ställs och att uppföljning sker av biträdet.

Dataskyddsombudet tillser att personalen utbildas och genomför såväl stickprover som årlig sammanställning till styrelsen.

Vid incidenter meddelas riskhanteringsansvarig, VD och dataskyddsombud. Dataskyddsombudet handhar sedan frågan och samtliga inblandade deltar i den utredning som sker.

4 Personuppgift, särskilda kategorier, brott, personnummer

Med personuppgift avses all information som direkt eller indirekt kan hänföras till en fysisk person som är i livet t.ex. namn, personnummer, adress, e-postadress, nätidentifierare, nummerskylt, bilder, kundnummer, lägenhetsnummer m.m.

Avidentifierade, avlidna eller juridiska personer utgör således inte personuppgifter.

En del personuppgifter är s.k. särskilda kategorier av personuppgifter (känsliga personuppgifter) för vilka särskilda regler gäller. Dessa uppgifter är:

- ras eller etniskt ursprung
- politiska åsikter
- religiös eller filosofisk övertygelse
- medlemskap i fackförening

- behandling av genetiska uppgifter
- biometriska uppgifter
- uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning ska vara förbjuden.

Vidare finns särskilda regler för:
- personuppgifter som rör fällande domar i brottmål samt överträdelser
- personnummer

Rättsinformation:
- *Artikel 4.13-4.15, 9, 10, 87*
- *Skäl 34, 35, 51*

5 Behandling av personuppgifter

Med behandling avses 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.

Behandlingen kan således vara helt automatiserad (allt sker elektroniskt), delvis automatiserad (manuell insamling och automatiserad behandling) eller manuell (om det utgör en del av ett register, ex. ett sökbart kartotek).

Rättsinformation:
- *Artikel 2.1, 4.1-4.2*
- *Skäl 15, 26-30*

5.1 Allmänna krav på behandling

All behandling av personuppgifter måste uppfylla de grundläggande principer som anges i dataskyddsförordningen.

Laglighet, korrekthet och öppenhet
Personuppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Kravet på att behandlingen av personuppgifter ska vara laglig innebär bland annat att det måste finnas en rättslig grund för behandlingen.

Att personuppgifter ska behandlas på ett öppet sätt i förhållande till den registrerade innebär bland annat att det ska vara klart och tydligt för denne hur hans eller hennes personuppgifter samlas in och i övrigt behandlas. De registrerade måste därför få information om behandlingen som är både lättillgänglig och formuleras med ett klart och tydligt språk.

Med korrekthet menas att personuppgifterna ska vara korrekta och uppdaterade samt ska rättas eller raderas om de är felaktiga.

Rättsinformation:

- *Artikel 5.1a*
- *Skäl 39, 58, 60*

Ändamålsbegränsning
Personuppgifter ska bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Det innebär att den som ska behandla personuppgifter måste ha ändamålen klara för sig redan innan insamlingen av personuppgifter börjar. Personuppgifterna får sedan inte behandlas på ett sätt som är oförenligt med dessa ändamål. De på förhand fastställda ändamålen är med andra ord det som sätter ramarna för behandlingen. Ändamålen ska dokumenteras skriftligt och den registrerade ska få information om ändamålen både när uppgifterna samlas in och annars när denne begär det. Om de insamlade personuppgifterna senare ska behandlas för andra ändamål som är förenliga med de ursprungliga ändamålen måste de registrerade också informeras om detta.

De insamlade personuppgifterna får behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål utan att det anses oförenligt med de ursprungliga ändamålen om det finns lämpliga skyddsåtgärder för de registrerades rättigheter.

Rättsinformation:
- *Artikel 5.1b, 6.4, 13.3, 14.4, 89.1.*
- *Skäl 39 och 50.*

Uppgiftsminimering
Principen om uppgiftsminimering innebär att personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas. Det är med andra ord inte tillåtet att samla in personuppgifter för obestämda framtida behov. Insamlade personuppgifter får inte heller behandlas om de till exempel är så gamla att de inte längre är relevanta för de ursprungliga ändamålen.

Lagringsminimering
Personuppgifter får inte sparas, det vill säga. 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.

När personuppgifterna inte längre behövs för de ändamålen ska de raderas eller avidentifieras. För att säkerställa att personuppgifter inte sparas längre än nödvändigt bör den som behandlar personuppgifter införa tidsfrister och rutiner för radering eller avidentifiering.

De insamlade personuppgifterna får lagras under längre tid för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål om det finns lämpliga skyddsåtgärder för de registrerades rättigheter.

Rättsinformation:
- *Artikel 5.1e*
- *Skäl 39*

Integritet och konfidentialitet

Personuppgifterna ska skyddas bland annat mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Den som behandlar personuppgifter ska därför vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna.

Rättsinformation:

- *Artikel 5.1f*
- *Artikel 32*
- *Skäl 39 och 83*

Ansvarsskyldighet
Den som behandlar personuppgifter ansvarar för att principerna om personuppgiftsbehandling följs och måste kunna visa på vilket sätt man följer dem. Det finns flera sätt att visa detta, till exempel genom att ha tydlig information till de registrerade, att dokumentera de behandlingar som pågår i organisationen och de överväganden man har gjort samt att ha dokumenterade interna riktlinjer för dataskyddet (en dataskyddspolicy). Att utse ett dataskyddsombud som bidrar till organisationens efterlevnad av förordningen och de interna riktlinjerna kan också vara ett sätt att uppfylla kravet på ansvarsskyldighet.

Rättsinformation:

- *Artikel 5.2*
- *Skäl 82*

5.2 Rättslig grund för behandling

För att det ska vara tillåtet att behandla personuppgifter måste det alltid finnas ett stöd i dataskyddsförordningen, en så kallad rättslig grund. En sådan rättslig grund är t.ex. samtycke från den registrerade, nödvändig för att fullgöra ett avtal med den registrerade, fullgöra en rättslig förpliktelse, skydda den registrerades grundläggande intressen, fullgöra en uppgift av allmänt intresse, samt efter en intresseavvägning.

Förutom kravet på rättslig grund måste behandlingen också uppfylla övriga bestämmelser i förordningen. Kom ihåg att möjligheten att behandla personuppgifter begränsas av de grundläggande principerna för behandling av personuppgifter och de ytterligare krav som tillkommer för vissa typer av personuppgifter, till exempel känsliga personuppgifter och uppgifter om lagöverträdelser.

För särskilda kategorier av personuppgifter (känsliga uppgifter), domar avseende brottmål, personnummer samt barn finns särskilda krav, se nedan.

5.2.1 Vanliga personuppgifter

En behandling av ”vanliga personuppgifter” är laglig om den följer vad som stadgas i Förordningens Artikel 6. Där räknas ett antal grunder upp varav de nedan är aktuella för bolaget med hänsyn tagen till dess verksamhet.

- Den registrerade har lämnat sitt samtycke.

- Behandlingen är nödvändig för att fullgöra ett avtal i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.

- Behandlingen är nödvändig för att fullgöra en rättslig förpliktelse som åvilar den personuppgiftsansvarige.

- Behandlingen är nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter, särskilt när den registrerade är ett barn.

- Arkivändamål

Rättsinformation:
- *Artikel 6*
- *Skäl 40-49*
- *Lag med kompletterande bestämmelser till EU:s dataskyddsförordning 2 kap 1-4§§*

5.2.2 Särskilda kategorier (känsliga) personuppgifter

Behandling av särskilda kategorier av personuppgifter är som utgångspunkt förbjudna, men får dock ske enligt Förordningens Artikel 9, varav följande är aktuella för bolaget med hänsyn tagen till dess verksamhet.

- Den registrerade har uttryckligen lämnat sitt samtycke (får inte ske konkludent).

- Behandlingen är nödvändig för att den personuppgiftsansvarige eller den registrerade ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter inom arbetsrätten och på områdena social trygghet och socialt skydd, i den omfattning detta är tillåtet enligt unionsrätten eller medlemsstaternas nationella rätt eller ett kollektivavtal som antagits med stöd av medlemsstaternas nationella rätt, där lämpliga skyddsåtgärder som säkerställer den registrerades grundläggande rättigheter och intressen fastställs.

- Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade.

- Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet.

- Behandlingen är nödvändig av skäl som hör samman med förebyggande hälso- och sjukvård och yrkesmedicin, bedömningen av en arbetstagares arbetskapacitet, medicinska diagnoser, tillhandahållande av hälso- och sjukvård, behandling, social omsorg eller förvaltning av hälso- och sjukvårdstjänster och social omsorg och av deras system, på grundval av unionsrätten eller medlemsstaternas nationella rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att de villkor och skyddsåtgärder som avses i punkt 3 är uppfyllda.

- Behandlingen är nödvändig för arkivändamål av allmänt intresse.

Rättsinformation:
- *Artikel 9*
- *Skäl 34, 35, 51-56.*

- *Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 3 kap. 1-7§§*

5.2.3 Personuppgifter som rör fällande domar i brottmål samt överträdelser

Behandling av personuppgifter som rör fällande domar i brottmål och överträdelser eller därmed sammanhängande säkerhetsåtgärder får endast utföras under kontroll av myndighet

Bolaget kan dock hantera personuppgifter avseende brottmål om det är nödvändigt för att:

- rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras
- en rättslig förpliktelse enligt lag eller förordning ska kunna fullgöras
- behandlingen är nödvändig för kontroll av att jävssituation inte föreligger i advokatverksamhet eller annan juridisk verksamhet
- behandlingen avser endast enstaka uppgift som är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras i ett enskilt fall
- uppgifterna avser personer i nyckelpositioner eller ledande ställning inom det egna bolaget eller koncernen och det är sakligt motiverat att behandla uppgifterna i särskilt inrättade rapporteringskanaler för att utreda om personen ifråga varit delaktig i allvarliga oegentligheter som rör bokföring, intern bokföringskontroll, revision, bekämpande av mutor, brottslighet inom bank- och finansväsen, eller andra allvarliga oegentligheter som rör organisationens vitala intressen eller enskildas liv och hälsa.

Rättsinformation:
- *Artikel 10*
- *Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 3 kap. 8-9 §§*
- *Förordning (2018:219) med kompletterande bestämmelser till EU:s dataskyddsförordning. §§ 5-6*
- *DIFS 2018:2*

5.2.4 Identifikationsnummer (personnummer)

Användning av personnummer får endast ske i följande fall:

- Den registrerade har samtyckt
- När det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av säker identifiering eller annat beaktansvärt skäl.

För bolagets del torde det i första hand röra sig om vikten av säker identifiering vid skadereglering av personskador, hantering av arbetstagare, skadelidande vid ansvarsskador m.m. Om ett ärende kan hanteras utan användande av personnummer ska så ske.

Rättsinformation:

- *Artikel 87*
- *Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 3 kap. §§10-11*

5.3 Samtycke

Med samtycke avses 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.

Frivillighet
Ett frivilligt samtycke innebär att den registrerade har en genuin eller fri valmöjlighet, kan vägra eller ta tillbaka samtycke. Således får man inte göra ett avtal eller tjänst beroende av samtycke om behandling av personuppgifter om inte detta är nödvändigt för avtalet eller tjänsten.

Specifik
Samtycket måste vara specifikt för ett visst ändamål som är uttryckligt angivet, berättigat i förhållande till ändamålet, vara begränsat och inte generellt samt ha gjorts uppenbar innan behandlingen inleds.

Informerat
För att samtycket ska vara informerat ska den registrerade ha fått information enligt XX nedan samt ha informerats om följderna av att inte ge samtycke. Informationen ska lämnas innan behandling sker samt även vid ändrad behandling.

Informationen ska vara klar och tydlig, den ska särskiljas från andra frågor och inte vara invävd i annan information, vara begriplig, lättillgänglig och anpassad efter mottagaren. Således får inte informationen ex. vara en hänvisning till allmänna villkor som inte tillhandahålls vid tillfället för samtycke och där den registrerade inte kan välja att godta villkoren eller inte.

Otvetydig viljeyttring
Med en otvetydig viljeyttring avses en aktiv handling från den registrerade, muntlig, skriftlig, elektronisk eller konkludent (dvs genom sitt handlande, ex ansöker om skadeersättning och därvid lämnar uppgifter, OBS GÄLLER EJ KÄNSLIGA UPPGIFTER, se ovan).

En aktiv handling är ex:

- Samtycke på pappersblankett
- Kryssa i ruta på papper eller elektroniskt
- Klicka på länk online
- Välja mellan tydliga ja/nej alternativ
- Välja tekniska inställningar

- Svara på e-postmeddelande
- Svara på muntlig begäran
- Att aktivt ansöka eller efterfråga något och då lämna personuppgifter

Handlingar som inte är aktiva är ex:

- Tysta samtycken (om du inte säger nej så godkänner du)
- Hypotetiska samtycken (X vill nog för det är bra….)
- Förkryssade rutor
- Standardinställningar

För att det ska vara en otvetydig viljeyttring måste den registrerade faktiskt förstå att det handlar om ett samtycke, varför bolaget måste ta hänsyn till behandlingens art, ändamål, kategori av personuppgifter och vem som är registrerad (ålder, mental förmåga att förstå).

Bolaget ska sträva efter skriftligt samtycke i möjligaste mån, genom egna skadeanmälnings-blanketter eller genom dokumentering av konkludenta handlingar av registrerade, ex spara mail, spontananmälningar, förfrågningar m.m.

Rättsinformation:
- *Artikel 7 och 8.*
- *Skäl 32, 42 och 43.*

5.3.1 Återkallelse

Den registrerade har rätt att när som helst återkalla sitt samtycke, lika lätt och i samma form som de lämnades.

Efter ett återkallande får inte ytterligare personuppgifter samlas in eller behandlas, redan insamlade uppgifter inte uppdateras eller kompletteras.

Behandling får dock fortsatt ske med de personuppgifter som lämnats för samma ändamål.

Rättsinformation:
- *Artikel 7.3*

5.3.2 Barns samtycke avseende informationssamhällets tjänster

Med informationssamhällets tjänster avses alla tjänster enligt definitionen i artikel 1.1 b i Europaparlamentets och rådets direktiv (EU) 2015/1535. Det rör sig om bland annat olika sociala medier, såsom till exempel bloggar, internetforum, webbplatser för videoklipp, chattprogram och sociala nätverk. Även onlinespel och olika applikationer (appar) med spel eller annat innehåll kan omfattasav definitionen.

När det gäller personuppgiftsbehandling som inte sker i samband med att informations-samhällets tjänster erbjuds får en bedömning, liksom tidigare, göras i varje enskilt fall av den registrerades förmåga att förstå innebörden av ett lämnat samtycke.

Vid erbjudande av informationssamhällets tjänster direkt till ett barn är behandling av personuppgifter som rör ett barn tillåten om barnet är minst 13 år.

Om barnet är under 13 år sådan behandling vara tillåten endast om och i den mån samtycke ges eller godkänns av den person som har föräldraansvar för barnet.

Med hänsyn till bolagets verksamhet torde inte några informationssamhällets tjänster bli aktuella för vår handläggning.

Rättsinformation:
- *Artikel 8*
- *Skäl 32, 38, 42-43.*
- *Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 2 kap 4§*

5.3.3 Dokumentation av samtycke

Den som behandlar personuppgifter med stöd av ett samtycke måste kunna visa att ett giltigt samtycke har lämnats av den registrerade. Personuppgiftsansvarig ska dokumentera samtycket för att kunna visa att det uppfyller de krav som gällande rätt kräver genom ett verifierbart bevis:

- Vem har samtyckt (t.ex namn, e-postadress, sessions id)
- När gavs samtycket (kopia av daterat dok, loggar m tidsangivelse etc)
- Vilken information lämnades (kopia på informationstext, policy m.m.)
- Hur samtycket lämnades (t.ex uppgifter i formulär)
- Om samtycket återkallats (t.ex. tidpunkt för återkallelse)

Rättsinformation:
- *Artikel 5*
- *Skäl 42*

6 Rättigheter för den registrerade

De personer vars personuppgifter behandlas, de registrerade, har ett antal rättigheter enligt dataskyddsförordningen. Dessa rättigheter innebär i korthet att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Därför har de bland annat rätt att i vissa fall få sina uppgifter rättade, raderade eller blockerade, eller att få ut eller flytta sina uppgifter. De registrerades rättigheter har utökats, förstärkts och specificerats i dataskyddsförordningen jämfört med personuppgiftslagen. Mer information om rättigheterna finns här nedan.

6.1 Allmänt avseende information och kontakter

Den personuppgiftsansvarige ska vidta lämpliga åtgärder för att till den registrerade tillhandahålla information och kommunikation, vilken avser behandling, i en koncis, klar och

tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk, i synnerhet för information som är särskilt riktad till barn.

Rättsinformation:

- *Artikel 12*
- *Skäl 58-64*

6.1.1 Form av utlämnande och kontakt

Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. (Om den registrerade lämnar begäran i elektronisk form, ska informationen om möjligt tillhandahållas i elektronisk form, om den registrerade inte begär något annat).

Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt.

6.1.2 Tid för utlämnande och kontakt (eller vägran att utlämna)

Den personuppgiftsansvarige ska på begäran utan onödigt dröjsmål, senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits enligt nedan. Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden.

Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från det att begäran mottagits samt ange orsakerna till förseningen.

Om den personuppgiftsansvarige inte vidtar åtgärder på den registrerades begäran, ska den personuppgiftsansvarige utan dröjsmål och senast en månad efter att ha mottagit begäran informera den registrerade om orsaken till att åtgärder inte vidtagits och om möjligheten att lämna in ett klagomål till en tillsynsmyndighet och begära rättslig prövning.

6.1.3 Kostnader

Information som tillhandahålls och all kommunikation och samtliga åtgärder som vidtas ska tillhandahållas kostnadsfritt.

Om begäranden från en registrerad är uppenbart ogrundade eller orimliga, särskilt på grund av deras repetitiva art, får den personuppgiftsansvarige antingen:

- ta ut en rimlig avgift som täcker de administrativa kostnaderna för att tillhandahålla den information eller vidta den åtgärd som begärts, eller

- vägra att tillmötesgå begäran.

Det åligger den personuppgiftsansvarige att visa att begäran är uppenbart ogrundad eller orimlig. Detta ska dokumenteras.

6.1.4 Kontroll av identitet

Identiteten fastställs genom de uppgifter som lämnas i ansökan, e-mail, eller muntligt. Om muntlig info ska ske skickas brev till folkbokföringsadressen med kodord eller så baseras det

på information från tidigare kontakter som är unika i ärendet och som endast registrerad vet om (ex vad som står i skadeanmälan).

Bolaget skickar f.n. brev eller usb till folkbokföringsadressen vid lämnande av information eller registerutdrag, alternativt kan krypterad epost användas (se stadens regler för epost och kryptering)

6.1.5 Offentlighet samt begränsning av information

Reglerna om offentliga handlingar och sekretess (OSL) har företräde före de avseende dataskyddsreglerna, varför en begäran om offentlig handling ska handhas enligt OSL. Skyldigheten att lämna ut handlingar gäller dock inte elektronisk form, varför dataskyddsreglerna gäller för sådana handlingar.

Vid begäran om offentlig handling informeras dataskyddsombudet och ärendet lämnas till bolagsjuristen.

Bolaget informerar i färdiga texter om att behandling kan ske för OSL och registrerad behöver därför inte meddelas när någon begär ut offentliga handlingar.

Får man inte lämna ut handlingar pga sekretess gäller detta före förordningen.,

Rättsinformation:

- *Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning 1 kap §§7-8.*
- *Offentlighet- och sekretesslagen (2009:400) 10 kap. 27§ samt 21 kap. 7§.*

6.2 Information

Den registrerade har rätt att få information när hans eller hennes personuppgifter behandlas. Information om personuppgiftsbehandlingen ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det. Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar ett dataintrång eller liknande (en personuppgiftsincident) hos den personuppgiftsansvarige och det finns risk för till exempel identitetsstöld eller bedrägeri.

Då bolaget endast handhar personuppgifter för handläggning av administration, skadereglering och försäkringar så finns färdiga texter på hemsidan, i skadeanmälnings-dokument samt i e-post. De är i dessa fall direkt nåbara för registrerad och någon särskild information behöver inte skickas ut. I andra fall samt vid begäran från registrerad och registerutdrag tillämpas reglerna nedan.

6.2.1 Information insamlad från den registrerade

Information från den registrerade ska vara skriftligt, elektroniskt eller muntligt på registrerads begäran (endast om identiteten kan fastställas) och ska lämnas när den samlas in. Information som den registrerade redan har behöver inte lämnas ut.

Följande information ska lämnas:

- Identitet och kontaktuppgifter för den personuppgiftsansvarige

- Kontaktuppgifter för dataskyddsombudet

- Ändamålen med behandlingen

- Den rättsliga grunden för behandlingen.

- Mottagarna eller kategorier av mottagare

- Eventuella överföringar av personuppgifter till ett tredjeland, huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.

- Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.

- Registrerads rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.

- Rätt att återkalla samtycke utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
- Rätten att inge klagomål till en tillsynsmyndighet

- Förekomsten av automatiserat beslutsfattande

Rättsinformation:
- *Artikel 13*
- *Skäl 58-64*
- *Artikel 29-gruppen, Riktlinje om*

6.2.2 Information insamlad från annan registrerade

Information från den registrerade ska vara skriftligt, elektroniskt eller muntligt på registrerads begäran (endast om identiteten kan fastställas, se dock OSL).

Bolaget skickar f.n. brev eller usb till folkbokföringsadressen vid lämnande av information eller registerutdrag, alternativt kan krypterad epost användas (se stadens regler för epost och kryptering)

Informationen ska lämnas ut:

- inom en rimlig period efter det att personuppgifterna har erhållits, dock senast inom en månad

- om personuppgifterna ska användas för kommunikation med den registrerade, senast vid tidpunkten för den första kommunikationen med den registrerade

- om ett utlämnande till en annan mottagare förutses, senast när personuppgifterna lämnas ut för första gången.

Undantag från utlämnande av information:

- Information som den registrerade redan har behöver inte lämnas ut.
- Om det är omöjligt eller är en oproportionerlig ansträngning
- Omöjliggör eller allvarligt försvårar målen med behandlingen (ex. utredning om bedrägeri)
- Lagstadgad tystnadsplikt

Följande information ska lämnas:

- Identitet och kontaktuppgifter för den personuppgiftsansvarige
- Kontaktuppgifter för dataskyddsombudet
- Ändamålen med behandlingen
- Den rättsliga grunden för behandlingen.
- Kategorier av personuppgifter*
- Mottagarna eller kategorier av mottagare
- Eventuella överföringar av personuppgifter till ett tredjeland, huruvida ett beslut av kommissionen om adekvat skyddsnivå föreligger eller saknas eller, hänvisning till lämpliga eller passande skyddsåtgärder och hur en kopia av dem kan erhållas eller var dessa har gjorts tillgängliga.
- Den period under vilken personuppgifterna kommer att lagras eller, om detta inte är möjligt, de kriterier som används för att fastställa denna period.
- Registrerads rätt att av den personuppgiftsansvarige begära tillgång till och rättelse eller radering av personuppgifter eller begränsning av behandling som rör den registrerade eller att invända mot behandling samt rätten till dataportabilitet.
- Rätt att återkalla samtycke utan att detta påverkar lagligheten av behandlingen på grundval av samtycket, innan detta återkallades.
- Rätten att inge klagomål till en tillsynsmyndighet
- Personuppgifternas ursprung*
- Förekomsten av automatiserat beslutsfattande

Rättsinformation:

- *Artikel 14*
- *Skäl 58-64*

6.2.3 Registerutdrag – information på begäran av registrerad

Den registrerade har rätt att av den personuppgiftsansvarige få bekräftelse på huruvida personuppgifter som rör honom eller henne håller på att behandlas och i så fall få tillgång till personuppgifterna samt information enligt nedan. (Se även Dataportabilitet nedan.)

Den personuppgiftsansvarige ska förse den registrerade med en kopia av de personuppgifter som är under behandling. För eventuella ytterligare kopior som den registrerade begär får den personuppgiftsansvarige ta ut en rimlig avgift på grundval av de administrativa kostnaderna.

Informationen ska tillhandahållas skriftligt, eller i någon annan form, inbegripet, när så är lämpligt, i elektronisk form. Om den registrerade begär det får informationen tillhandahållas muntligt, förutsatt att den registrerades identitet bevisats på andra sätt. Om den registrerade gör begäran i elektronisk form ska informationen tillhandahållas i ett elektroniskt format som är allmänt använt, om den registrerade inte begär något annat.

Bolaget skickar f.n. brev eller usb till folkbokföringsadressen. Om muntlig info ska ske skickas brev till folkbokföringsadressen med kodord som kvitteras i samtalet.

Information kan även skickas via e-post om den bifogade filen är krypterad genom Microsoft Office version 2007 eller senare förutsatt att dokumentet sparas i docx-format.

Den personuppgiftsansvarige ska på begäran utan onödigt dröjsmål och under alla omständigheter senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits. Denna period får vid behov förlängas med ytterligare två månader, med beaktande av hur komplicerad begäran är och antalet inkomna begäranden. Den personuppgiftsansvarige ska underrätta den registrerade om en sådan förlängning inom en månad från det att begäran mottagits samt ange orsakerna till förseningen.

Följande information ska lämnas:

- Ändamålen med behandlingen. (Se registerförteckningen)

- De kategorier av personuppgifter som behandlingen gäller. (Se registerförteckningen)

- De mottagare eller kategorier av mottagare till vilka personuppgifterna har lämnats eller ska lämnas ut, särskilt mottagare i tredjeländer eller internationella organisationer och rätt till information om de lämpliga skyddsåtgärder som vidtas (Se registerförteckingen)

- 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. (Se registerförteckningen)

- Förekomsten av rätten att av den personuppgiftsansvarige begära rättelse eller radering av personuppgifterna eller begränsningar av behandling av personuppgifter som rör den registrerade eller att invända mot sådan behandling. (Se information på hemsidan)

- Rätten att inge klagomål till en tillsynsmyndighet. (Se information på hemsidan)

- Om personuppgifterna inte samlas in från den registrerade, all tillgänglig information om varifrån dessa uppgifter kommer. (Se registerförteckningen)

- Förekomsten av automatiserat beslutsfattande.

Rättsinformation:
- *Artikel 15*
- *Skäl 58-64*

6.3 Rättelse

Registrerad har rätt att utan dröjsmål få felaktiga uppgifter rättade och kompletterade. Personuppgiftsansvarig ska kontrollera identiteten och dokumentera ändringen eller kompletteringen.

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om eventuella rättelser om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Rättsinformation:
- *Artikel 16,19.*
- *Skäl 65*

6.4 Radering

Registrerad har rätt att utan dröjsmål få sina personuppgifter raderade på de grunder som anges nedan med beaktande av undantagen. Om uppgifterna offentliggjorts ska den personuppgiftsansvarige underrätta andra personuppgiftsansvariga/biträden att radera eventuella länkar till, eller kopior eller reproduktioner av dessa personuppgifter.

Med anledning av att bolaget omfattas av offentlighets- och sekretesslagen samt arkivlagen ska radering alltid diskuteras med och utredas av dataskyddsombudet samt stadens generella och bolagets specifika bevarandehandling/gallringsbeslut kontrolleras.

Personuppgiftsansvarig ska kontrollera identiteten och dokumentera raderingen.

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om radering av personuppgifter om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Grunder för radering:

- Uppgifterna är inte längre nödvändiga för de ändamål för vilka de samlats in

- Samtycke återkallas och det inte finns någon annan rättslig grund
- Olaglig behandling
- Rättslig förpliktelse
- Insamling har skett i samband med erbjudande av informationssamhällets tjänster till barn.

Undantag från radering:

- Utövande av yttrande- och informationsfrihet
- Rättslig förpliktelse
- Arkivändamål
- Fastställa, göra gällande eller försvara rättsliga anspråk.

Rättsinformation:
- *Artikel 17,19*
- *Skäl 65-66*

6.5 Begränsning av behandling

Registrerad har rätt att kräva begränsning av behandlingen om:

- Registrerad bestrider personuppgifternas korrekthet, under en tid som ger den personuppgiftsansvarige en möjlighet att kontrollera om personuppgifterna är korrekta.
- Behandlingen är olaglig och den registrerade motsätter sig att personuppgifterna raderas och i stället begär en begränsning av deras användning.
- Den personuppgiftsansvarige inte längre behöver personuppgifterna för ändamålen med behandlingen men den registrerade behöver dem för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.
- Den registrerade har invänt mot behandling genom berättigat intresse, direkt marknadsföring i väntan på kontroll av huruvida den personuppgiftsansvariges berättigade skäl väger tyngre än den registrerades berättigade skäl.

Om behandlingen har begränsats får sådana personuppgifter, med undantag för lagring, endast behandlas med den registrerades samtycke eller för att fastställa, göra gällande eller försvara rättsliga anspråk eller för att skydda någon annan fysisk eller juridisk persons rättigheter eller för skäl som rör ett viktigt allmänintresse för unionen eller för en medlemsstat.

En registrerad som har fått behandling begränsad ska underrättas av den personuppgifts-ansvarige innan begränsningen av behandlingen upphör.

Den personuppgiftsansvarige ska underrätta varje mottagare till vilken personuppgifterna har lämnats ut om begränsningar av behandling som om inte detta visar sig vara omöjligt eller medföra en oproportionell ansträngning. Den personuppgiftsansvarige ska informera den registrerade om dessa mottagare på den registrerades begäran.

Personuppgiftsansvarig ska kontrollera identiteten och dokumentera ändringen eller kompletteringen.

Rättsinformation:
- *Artikel 4.3, 18, 19*
- *Skäl 67*

6.6 Dataportabilitet

Den registrerade har i vissa fall rätt att få ut de personuppgifter som rör honom eller henne i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig (direkt från en personuppgiftsansvarig till en annan, när detta är tekniskt möjligt).

Personuppgiftsansvarig ska kontrollera identiteten och dokumentera.

F.n. utges personuppgifterna genom att usb sänds till folkbokföringsadressen i word, excel eller excelformat, alternativt krypterat via epost (se stadens regelverk avseende epost).

Förutsättningar för dataportabilitet:

- Avser endast personuppgift som den registrerade har tillhandahållit den personuppgiftsansvarige

- Behandlingen grundas på samtycke

- Behandlingen är automatiserad

- Dataportabilitet får inte påverka andras rättigheter på ett ogynnsamt sätt.

Rättsinformation:
- *Artikel 20*
- *Skäl 68*
- *Artikel 29-gruppen, Riktlinjer om rätten till dataportabilitet*

6.7 Invändningar

Invändningar av den registrerade mot behandling av personuppgifter får ske enligt nedan.

Personuppgiftsansvarig ska kontrollera identiteten och dokumentera hanteringen i skadeakt/system.

Rättsinformation:
- *Artikel 21*
- *Skäl 69-70*

6.7.1 Behandling pga. allmänt intresse eller intresseavvägning

Den registrerade har rätt att när som helst göra invändningar mot behandling av personuppgifter avseende honom eller henne som grundar sig på allmänt intresse eller berättigat intresse (se laglighet ovan) inbegripet profilering som grundar sig på dessa bestämmelser.

Den personuppgiftsansvarige får inte längre behandla personuppgifterna såvida denne inte kan påvisa:

- Tvingande berättigade skäl för behandlingen som väger tyngre än den registrerades intressen, rättigheter och friheter

- Fastställande, utövande eller försvar av rättsliga anspråk.

6.7.2 Direkt marknadsföring

Om personuppgifterna behandlas för direkt marknadsföring har registrerade rätt att när som helst invända mot behandling av personuppgifter som avser honom eller henne för sådan marknadsföring, vilket inkluderar profilering i den utsträckning som denna har ett samband med sådan direkt marknadsföring.

Om den registrerade invänder mot behandling för direkt marknadsföring ska personuppgifterna inte längre behandlas för sådana ändamål.

Senast vid den första kommunikationen med den registrerade ska den rätt som avses ovan uttryckligen meddelas den registrerade och redovisas tydligt, klart och åtskilt från eventuell annan information.

6.7.3 Informationssamhällets tjänster

När det gäller användningen av informationssamhällets tjänster får den registrerade utöva sin rätt att göra invändningar på automatiserat sätt med användning av tekniska specifikationer.

6.7.4 Behandling pga. vetenskapliga, historiska eller statistiska ändamål

Om personuppgifter behandlas för vetenskapliga eller historiska forskningsändamål eller statistiska ändamål har den registrerade, av skäl som hänför sig till hans eller hennes specifika situation, rätt att göra invändningar mot behandling av personuppgifter avseende honom eller henne om inte behandlingen är nödvändig för att utföra en uppgift av allmänt intresse.

6.8 Automatiserat individuellt beslutsfattande

Den registrerade har rätt att inte bli föremål för ett beslut som enbart grundas på automatiserad behandling. Behandlingen får dock ske om det är nödvändigt för ingående eller fullgörande av avtal, samtycke eller enligt gällande rätt. För särskilda kategorier av personuppgifter får automatiserat beslutsfattande endast ske efter registrerads samtycke.

Den personuppgiftsansvarige ska genomföra lämpliga åtgärder för att säkerställa den registrerades rättigheter, friheter och rättsliga intressen, åtminstone rätten till personlig kontakt med den personuppgiftsansvarige för att kunna utrycka sin åsikt och bestrida beslutet.

Rättsinformation:

- *Artikel 22, 13.2 f, 14.2g,*

- *Skäl 71,72*

7 Registerförteckning

Personuppgiftsansvarig och personuppgiftsbiträde ska föra skriftligt/elektroniskt register över behandling som utförs av dem.

Bolaget har ett register för all sina behandlingar under G/2Verksamhetsstöd/2.5 Kommunicera/PUL.

Rättsinformation:
- *Artikel 30*
- *Skäl 82*

7.1 Registerförteckning personuppgiftsansvarig

Följande uppgifter ska finnas i registret:

- Namn och kontaktuppgifter på personuppgiftsansvariga och dataskyddsombud
- Ändamålen med behandlingen
- Kategorier av registrerade
- Kategorier av personuppgifter
- Kategorier av mottagare
- Överföringar till tredjeland och vidtagna säkerhetsåtgärder
- Tidsfrister för radering av uppgifter
- Beskrivning av tekniska och organisatoriska säkerhetsåtgärder

7.2 Registerförteckning personuppgiftsbiträde

Följande uppgifter ska finnas i registret:

- Namn och kontaktuppgift för personuppgiftsbiträdena och personuppgiftsansvarig samt dataskyddsombud
- Kategorier av behandling som utförs
- Överföringar till tredje land och skyddsåtgärder
- Beskrivning av tekniska och organisatoriska säkerhetsåtgärder

8 Säkerhet

8.1 Dataskydd

Inbyggt dataskydd (privacy by design) innebär att man tar hänsyn till integritetsskydds-reglerna redan när man utformar it-system och rutiner. Det är ett sätt att se till att kraven i dataskyddsförordningen uppfylls och att den registrerades rättigheter skyddas.

Kravet på dataskydd som standard (privacy by default) innebär i korthet att den som behandlar personuppgifter ska se till att personuppgifter i standardfallet inte behandlas i onödan. Det kan till exempel handla om att de förvalda inställningarna i en tjänst för sociala media är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas.

Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder.

Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

Exempel på åtgärder är:

- Pseudonymisering och kryptering
- Backup
- Regelbundna tester/undersökningar av teknik och organisation
- Säkerhetsnivå baserad på risken för oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst.
- Biträden och andra endast behandlar personuppgifter efter personuppgiftsansvarigs instruktion.

Vid bedömningen av lämplig säkerhetsnivå ska särskild hänsyn tas till de risker som behandling medför, i synnerhet från 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.

Bolagets principer för dataskydd framgår av Stockholm stads allmänna regler för dataskydd där krav ställs på åtkomst, loggning, rutiner, backup, kryptering, hantering m.m.:

- Riktlinje för informationssäkerhet
- Handbok för informationsklassificering.

- Kryptorekommendationer

Rättsinformation:
- *Artikel 25, 32,*
- *Skäl 78, 83*

8.2 Skyddade personuppgifter

Skyddade personuppgifter hanteras i enlighet med Stockholm stads riktlinje ”Stadsövergripande policy om skyddade personuppgifter”.

8.3 Personuppgiftsincident

Med personuppgiftsincident avses en incident 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,

Vid personuppgiftsincident ska riskhanteringsansvarig och dataskyddsombudet informeras och incidenten dokumenteras, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits.

Personuppgiftsbiträden ska utan onödigt dröjsmål informera personuppgiftsansvarig efter att ha fått vetskap om en personuppgiftsincident och därvid bistå personuppgiftsansvarig på alla sätt.

Dokumentering sker i bolagets incidentrapporteringssystem IA där även kopior på anmälningar och information ska biläggas.

Dataskyddsombudet beslutar i samråd med riskhanteringsansvarig och handläggare huruvida anmälan ska ske till tillsynsmyndigheten eller inte samt om registrerade ska informeras.

Rättsinformation:
- *Artikel 33,34.*
- *Skäl 85-88*

8.3.1 Anmälan till tillsynsmyndigheten

Incidenter ska anmälas till tillsynsmyndigheten såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter

Vid incident ska personuppgiftsansvarig anmäla incidenten till tillsynsmyndigheten utan onödigt dröjsmål, och om möjligt, inte senare än 72 timmar efter vetskap om incidenten. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.

Om och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.

I anmälan till tillsynsmyndigheten ska följande information ingå:

- Incidentens art

- Kategorier av och antalet registrerade som berörs
- Kategorier av och antalet personuppgiftsposter som berörs
- Namn och kontaktuppgifter till dataskyddsombudet samt andra relevant kontakter
- Konsekvensbedömning av incidenten
- Åtgärder som vidtagits eller kommer att vidtas för att åtgärda incidenten
- Åtgärder för att mildra incidentens potentiellt negativa effekter

8.3.2 Information till den registrerade

Om personuppgiftsincidenten sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige utan onödigt dröjsmål informera den registrerade om personuppgiftsincidenten.

Registrerad behöver inte informeras om något av följande uppfylls:

- Lämpliga tekniska och organisatoriska skyddsåtgärder vidtagits
- Åtgärder vidtagits som innebär att den ev höga risken inte uppstår
- Det skulle inbegripa en oproportionell ansträngning. I så fall ska i stället allmänheten informeras eller en liknande åtgärd vidtas genom vilken de registrerade informeras på ett lika effektivt sätt.

Den information som ska lämnas är densamma som till tillsynsmyndigheten, men ska var särskilt tydlig och klar.

9 Konsekvensbedömning av dataskydd

I vissa fall måste personuppgiftsansvarig genomföra en konsekvensbedömning innan behandling sker samt, om hög risk föreligger, samråda med tillsynsmyndigheten.

Konsekvensbedömningen ska dokumenteras under G/.

9.1 Konsekvensbedömning

Om en typ av behandling (särskilt med användning av ny teknik och med beaktande av dess art, omfattning, sammanhang och ändamål) sannolikt leder till en hög risk för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter. En enda bedömning kan omfatta en serie liknande behandlingar som medför liknande höga risker.

Konsekvensbedömning ska särskilt ske i följande fall:

- Systematisk och omfattande bedömning av fysiska personers personliga aspekter

- Behandling i stor omfattning av särskilda kategorier av uppgifter
- Behandling av personuppgifter fällande domar i brottmål eller överträdelser
- Systematisk övervakning av allmän plats i stor omfattning

Den personuppgiftsansvarige ska rådfråga dataskyddsombudet, om ett sådant utsetts, vid genomförande av en konsekvensbedömning avseende dataskydd.

Konsekvensbedömningen ska minst innehålla:

- Systematisk beskrivning av behandlingen
- Behandlingens syften
- Personuppgiftsansvariges berättigade intresse
- Bedömning av behovet och proportionaliteten med behandlingen
- Utvärdering av riskerna för de registrerades rättigheter och friheter
- Åtgärder för att hanteras riskerna (ex. skyddsåtgärder, säkerhetsåtgärder, rutiner)
- (om lämpligt inhämta registrerades synpunkter eller förklara varför så inte skett)

Den personuppgiftsansvarige ska vid behov genomföra en översyn för att bedöma om behandlingen genomförs i enlighet med konsekvensbedömningen avseende dataskydd åtminstone när den risk som behandlingen medför förändras.

Rättsinformation:
- *Artikel 35*
- *Skäl 89-95*
- *Artikel 29-gruppen, Riktlinjer för konsekvensbedömning*

9.2 Förhandssamråd

Den personuppgiftsansvarige ska samråda med tillsynsmyndigheten före behandling om en konsekvensbedömning avseende dataskydd visar att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar åtgärder för att minska risken.

Vid samråd ska följande information lämnas till tillsynsmyndigheten:

- i tillämpliga fall de respektive ansvarsområdena för de personuppgiftsansvariga, gemensamt personuppgiftsansvariga och personuppgiftsbiträden
- ändamålen med och medlen för den avsedda behandlingen
- de åtgärder som vidtas och de garantier som lämnas för att skydda de registrerades rättigheter och friheter enligt denna förordning,
- i tillämpliga fall kontaktuppgifter till dataskyddsombudet

- konsekvensbedömningen avseende dataskydd

- all annan information som begärs av tillsynsmyndigheten.

Rättsinformation:
- *Artikel 36*
- *Skäl 89-95*

10 Överföring till tredje land

Som huvudprincip är överföring av personuppgifter utanför EU/EES förbjuden. Överföring får dock ske om någon av följande förutsättningar föreligger:

- EU-kommissionen har beslutat att ett land har adekvat skyddsnivå

- Personuppgiftsansvarig/biträde har vidtagit lämpliga skyddsåtgärder

- Särskilda situationer

För bolagets del kan detta vara aktuellt om t.ex. servrar/backup finns i land utanför EU/EES.

Personuppgiftsansvarig ska rådfråga dataskyddsombudet innan behandling sker och utredningen ska dokumenteras som behandlingar i övrigt.

Rättsinformation:
- *Artikel 44-50*
- *Skäl 101-116, 169.*

10.1 Godkända länder

Se ”Commission decisions on the adequacy of the protection of personal data in third countries”

http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

10.2 Lämpliga skyddsåtgärder

I avsaknad av ett beslut om godkännande av ett land från EU-kommissionen kan personuppgiftsansvarig/biträde vidta nedan nämnda skyddsåtgärder, varvid överföring är tillåten.

Märka att en dator eller mobil som tas med utanför EU/EES utgör en tredjelandsöverföring.

Utan tillstånd från tillsynsmyndigheten:

- rättsligt bindande och verkställbart instrument mellan offentliga myndigheter

- bindande företagsbestämmelser (standarsklausuler BCR:s ska ha antagits eller godkänts av EU-kommissionen eller av en tillsynsmyndighet. Det behövs däremot inget särskilt tillstånd av tillsynsmyndighet för varje överföring.)

- standardiserade dataskyddsbestämmelser som antas av kommissionen
- standardiserade dataskyddsbestämmelser som antagits av en tillsynsmyndighet och godkänts av kommissionen
- godkänd uppförandekod
- godkänd certifieringsmekanism

Med tillstånd från tillsynsmyndigheten

- avtalsklausuler med personuppgiftsansvarig/biträde i tredjeland
- bestämmelser i administrativa överenskommelser mellan offentliga myndigheter

10.3 Särskilda situationer

I vissa situationer får personuppgifter överföras till tredjeland:

- Samtycke
- Fullgöra avtal eller åtgärder som föregår avtal på den registrerades begäran
- Fullgöra avtal eller åtgärder som föregår avtal i den registrerades intresse
- Allmänt intresse
- Nödvändig för rättsliga anspråk
- Intresseavvägning i enstaka fall (visst förfarande och dokumentation enligt Förordningen Artikel 49)

11 Outsourcing

Vid outsourcing ska krav på redovisning av hur personuppgifter behandlas finns i upphandlingsunderlaget. Det skall särskilt beaktas om motparten eller underleverantör behandlar data utanför EU/EES.

Upphandlingsunderlaget ska vidare innehålla krav på personuppgiftsbiträdet enligt 2.4 ovan.

Ansvarig för upphandlingen/ansvarig kontrollerar inom ramen för kontraktsuppföljning biträdets hantering av personuppgifter.

12 Dokumentation

Dokumentation av utredning, register, konsekvensbedömning, kontakter med tillsynsmyndigheten, personuppgiftsincidenter etc sker under

12.1 Utredning inför behandling

Utredning sparas under G/

12.2 Registerförteckning
Sparas under G/

12.3 Konsekvensbedömning
Sparas under G/

12.4 Incidenter
Sparas i IA samt kopia under G/

12.5 Utbildning
Sparas under G/

12.6 Intresseavvägning och godkännanden vid tredjelandsöverföring
Sparas under G/

12.7 Personuppgiftsbiträdesavtal m.m.
Sparas under G/ samt i avtalsdatabasen G/2/2.4/2.4.3/Avtal

Biträdets registerförteckningar sparas på samma sätt.

12.8 Dataportabilitet
Begäran och sändkvitto eller motsvarande sparas under G/

12.9 Samtycke
Sparas i den form den inkommit i det ärende den tillhör, ex. skadeakt.

12.10 Information
Sparas i den form den utgivits i det ärende den tillhör, ex skadeakt. Allmänna informationsskrifter för bolaget sparas under G/.

12.11 Registerutdrag
Begäran sparas i den form den inkom tillsammans med registerutdraget och bevis för utskick under G/.

12.12 Rättelse, radering, begränsning, invändningar
Begäran och åtgärd sparas under G/.

12.13 Rapporter
Sparas under G/.

13 Rapportering
Incidenter rapporteras av respektive handläggare till Riskhanteringsansvarig, Dataskyddsombud ,VD samt noteras i IA. Om en incident innebär att anmälan sker till tillsynsmyndigheten eller att registrerad informeras ska detta meddelas styrelsen av dataskyddsombudet.

Dataskyddsombudet ska årligen utfärda en rapport till VD och styrelse avseende bolagets personuppgiftsbehandling. I denna rapport ska följande redovisas:

- Bolagets behandlingar av personuppgifter (registerförteckningen)

- Genomförda kontroller

- Sammanställning över eventuella incidenter och hur dessa hanterats
- Rekommendationer som lämnats till verksamheten

- Eventuella konsekvensbedömningar som genomförts

14 Utbildning

Samtlig personal ska utbildas av dataskyddsombudet eller annan med erforderliga kunskaper i dessa riktlinjer och den process som gäller för företaget.

Utbildningen ska dokumenteras och ange när och var den ägts rum, vad den avsett, vilka som deltagit samt ska undertecknas av utbildare och deltagare.

Dokumentation sker under G/

15 Kontroll

Handläggare ansvarar för att kontroll enligt 2.3 ovan sker innan behandling utförs och av personuppgiftsbiträdens behandlingar och datasäkerhet samt riktlinjer inom ramen för kontraktsuppföljning.

Dataskyddsombudet kontrollerar att uppföljning sker av personuppgiftsbiträden, att tillgång till system är begränsat till de som behöver dem for sin handläggning, att regler kring personuppgifter finns vid upphandling, att system har informationsklassats och åtgärder vidtagits för datasäkerhet.

16 Klagomål

Den som anser att någon behandlar uppgifter om honom eller henne i strid med dataskyddsförordningen kan lämna in ett klagomål till Datainspektionen.

Datainspektionen tar del av alla klagomål och bedömer om tillsyn ska inledas och lämnar därefter besked till den som fört fram klagomålet. Datainspektionen måste meddela om tillsyn ska inledas eller inte inom tre månader efter att ha tagit emot klagomålet. Om den klagande inte får besked inom den tiden, kan han eller hon vända sig till domstol för att begära besked.

Bolaget har även en intern Riktlinje för hantering av klagomål” enligt regelverket för Solvens 2.

17 Lagring och gallring

Personuppgifter ska inte lagras längre eller i större omfattning än vad som är nödvändigt för ändamålet med behandlingen.

Som offentligt ägt bolag omfattas S:t Erik av arkivlagen. Regler för arkivering finns således i arkivlagen, arkivregler för Stockholms stad, riktlinjer för arkivregler i Stockholms stad samt att värdera och gallra information i Stockholms stad. Med ledning av dessa har bolaget en hanteringsanvisning under G/.

Generellt anpassar bolaget sin lagring/gallring som följer.

Försäkringsavtal	tills försäkringen upphör samt preskriptionstid (10 år från avtalets upphörande)
Skadereglering	preskriptionstid (10 år efterförsäkringsfall)
Bokföring	bokföringslagen, normalt 7 år
Avtal	preskriptionslagen (normalt 10 år)