Svensk Värdepappersservice

Instruktion för behandling av personuppgifter

Legal grund			
Dataskyddsförordning (EU) 2016/679, lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning			
Antagen av	**Datum för antagande**	**Datum f g version**	**Revideras för nytt fastställande**
Styrelsen	2025-05-08	2024-02-15	Årligen
Dokumentägare	**Upprättad av**	**Informationsklassificering**	
Dataskyddsombud	Funktion för riskhantering	Intern	

Ändringslogg

Datum	Författare	Version	Kommentar
2020–02-18	H Malm	2020.1	Ny Mall
2022-02-17	F Nilsson	2022.1	Årlig översyn
2024-02-15	F Nilsson	2024.1	Redaktionella ändringar.
2025-05-08	F Nilsson	2025.1	Redaktionella ändringar.

Innehåll

1 Bakgrund och syfte

Syftet med denna instruktion är att säkerställa att behandling av personuppgifter sker i enlighet med Europaparlamentets och rådets förordning (EU) 2016/679 (dataskyddsförordningen eller GDPR) och annan lagstiftning avseende dataskydd och skydd av personuppgifter. Instruktionen omfattar all behandling av personuppgifter, såväl strukturerade som ostrukturerade uppgifter.

Denna instruktion innehåller regler och riktlinjer för den behandling av personuppgifter som företas av Svensk Värdepappersservice i Stockholm AB (”Bolaget”) i egenskap av personuppgiftsansvarig.

2 Begrepp och definitioner

Begrepp/Förkortning	Förklaring
Anställd	Person som arbetar inom eller som uppbär ersättning eller har uppdrag för Bolaget, till exempel anställda, anlitade konsulter, anknutna ombud samt anställda hos anknutna ombud, styrelseledamöter och praktikanter.
Behandling av personuppgifter	Varje 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.
Den registrerade	Den fysiska person vars uppgifter behandlas som direkt eller indirekt kan identifieras av personuppgifterna.
Personuppgifter	All slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.
Personuppgifts-ansvarig	En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.
Dataskyddsombud (DPO)	Person som övervakar att Bolaget följer dataskyddsförordningen.
Personuppgifts-biträde	Personuppgiftsbiträde är en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsbiträdet finns alltid utanför den personuppgiftsansvariges organisation.
Personuppgifts-incident	En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.
GDPR	Dataskyddsförordningen (General Data Protection Regulation).
Regelverk	Dataskyddsförordningen samt annan tillämplig lag, förordning, tillsynsmyndigheters föreskrifter och allmänna råd, branschpraxis, god sed, interna policys, riktlinjer, instruktioner, rutiner samt processer.
IMY	Integritetsskyddsmyndigheten.

3 Bolaget och Dataskyddsförordningen

Den verksamhet som Bolaget bedriver innefattar till stor del behandling av personuppgifter, varför det är av största vikt att all behandling av personuppgifter utförs på ett sätt som är säkert och inte riskerar att göra intrång i de registrerades personliga integritet.

Syftet med instruktionen är att öka de anställdas kunskap om innehållet i GDPR och säkerställa förordningens efterlevnad i Bolagets verksamhet. God sed, god moral och hög etisk standard ska eftersträvas i all behandling av personuppgifter.

En förteckning (personuppgiftsregister) över de personuppgifter som behandlas inom Bolaget ska upprättas, dokumenteras och löpande uppdateras. För denna förteckning ansvarar DPO.

Det är styrelsen som bär det övergripande ansvaret kring GDPR-förordningen och vd som ansvarar för att de nödvändiga rutinerna kring det operativa genomförandet införs i bolaget. Alla anställda ansvarar för att innehållet i denna instruktion följs. Ett särskilt ansvar kan åvila enskild anställd eller avdelning för radering och gallring av personuppgifter. Detta framgår i sådana fall av Bolagets personuppgiftsregister.

4 Behandling av personuppgifter

4.1 Inledning

I huvudsak består Bolagets verksamhet av att ge råd till kunder om investeringar i finansiella instrument, granska och godkänna rådgivningsdokumentation och vidarebefordra order. Rådgivningen utförs av Bolagets anknutna ombud. Samtliga anställda hos ombudsbolaget som arbetar med den tillståndspliktiga verksamheten på uppdrag av Bolaget omfattas av denna instruktion och behandlas på samma vis som en anställd hos Bolaget i det avseendet.

Största delen av de personuppgifter som Bolaget behandlar sker inom ramen för ovan beskrivna tjänster samt för att kunna uppfylla gällande lagstiftning, exempelvis lag om värdepappersmarknaden och lag om åtgärder mot penningtvätt och finansiering av terrorism.

Bolaget behandlar personnummer när det är motiverat med hänsyn till ändamålet med behandlingen samt vikten av en säker identifiering. Det innebär att anställda ska undvika att slentrianmässigt använda personnummer i sammanhang då detta inte är nödvändigt med hänsyn till ändamålet med behandlingen samt vikten av en säker identifiering.

4.2 Principer för behandling

Enligt dataskyddförordningen måste all behandling av personuppgifter uppfylla ett antal grundläggande principer. Nedan redogörs för dessa principer samt hur Bolaget säkerställer att principerna följs.

1. Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt *(laglighet).* Bolaget säkerställer bland annat att en rättslig grund finns för all behandling som utförs hos bolaget.
2. Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål, samt får inte behandlas för något ändamål som är oförenligt med dessa ändamål *(ändamålsbegränsning).*
3. Personuppgifter ska vara adekvata, relevanta och inte fler än vad som är nödvändigt i förhållande till ändamålen med behandlingen *(uppgiftsminimering).* Finns inget klart ändamål med insamling av vissa uppgifter så ska uppgifterna inte samlas in. Endas uppgifter som behövs för att uppfylla ändamålet med behandlingen får behandlas.
4. Personuppgifter ska vara riktiga, och om nödvändigt, uppdaterade *(korrekthet)*. Bolaget samlar in nya och uppdaterar personuppgifter i den mån det är nödvändigt för administrationen av kundernas engagemang hos Bolaget. Uppgifterna inhämtas normalt

direkt från den registrerade, men i syfte att upprätthålla en god kund- och registervård kan Bolaget även komma att komplettera personuppgifterna genom inhämtande av uppgifter från offentliga och privata register, t ex uppdatering av adressuppgifter via Statens person- och adressregister (SPAR).

5. Personuppgifter får inte behandlas för en längre tid än vad som är nödvändigt med hänsyn till ändamålen för vilka personuppgifterna behandlas *(lagringsminimering).*
6. Personuppgifter får bara behandlas på ett sådant sätt som säkerställer lämpligt skydd för personuppgifter *(integritet och konfidentialitet).* Endast de anställd som behöver personuppgifterna för att kunna utföra sitt arbete ska ha tillgång till uppgifterna. Bolaget ska hantera personuppgifter på ett sätt som minimerar risken att de kommer att bli tillgängliga för obehöriga.
7. Den personuppgiftsansvarige ska ansvara för och kunna visa att dessa principer efterlevs *(ansvarsskyldighet).* Detta uppfylls bland annat genom dokumentation av beslut och åtgärder samt förteckning över Bolagets behandling av personuppgifter.

4.3 Dokumentation av behandling

All behandling av personuppgifter som inte är av tillfällig karaktär ska dokumenteras i Bolagets personuppgiftsregister. Nedan uppgifter ska, i förekommande fall, anges för varje enskild behandling.

- RegisterID.
- Situation för behandling av personuppgifter.
- Ändamål med behandling.
- Kategori av registrerad.
- Kategori av personuppgifter.
- Behörighet.
- Dokument/systemfunktion vari personuppgifter behandlas.
- Lagringsplats.
- Eventuell mappadress.
- Källa/insamling för personuppgifterna.
- Om personuppgifter delas externt.
- Laglig grund för behandling.
- Motivering intresseavvägning.
- Tidsfrist för radering.
- Gallringsrutin.
- Ansvarig för att gallringsrutin efterlevs.
- Informationskrav uppfyllt.
- Riskfaktorer.
- Skyddsåtgärder.
- Eventuella kommentarer.

4.4 Ny behandling

Inför varje ny behandling av personuppgifter ska nedan säkerställas.

- Att de grundläggande principerna följs (se 4.2).

- Att det finns en laglig grund för behandling (se 4.5.1).
- Att behandlingen, om den inte är tillfällig, dokumenteras i Bolagets personuppgiftsregister (se 4.3).
- Informera den registrerade (den fysiska person som behandlingen avser) om personuppgiftsbehandlingen.
- Att personuppgifterna skyddas.

4.5 Säkerställande av laglig och korrekt behandling av personuppgifter

4.5.1 Rättslig grund

För att behandling av personuppgifter ska kunna ske måste någon av nedan grunder vara uppfyllda. Om ingen av nedan grunder kan användas är behandling inte tillåten.

1. Den registrerade har lämnat sitt **samtycke** till att dennes personuppgifter behandlas.
2. Behandlingen är nödvändig för att **fullgöra ett avtal** som den registrerade är part i eller för att vidta förberedande åtgärder på den registrerades begäran inför ett avtal.
3. Behandlingen är nödvändig för att Bolaget ska uppfylla en **rättslig förpliktelse** som åvilar Bolaget.
4. Behandlingen är nödvändig för att **skydda intressen** som är av grundläggande betydelse för den registrerade eller för annan fysisk person.
5. Behandlingen är nödvändig för att utföra en uppgift av **allmänt intresse**.
6. Behandlingen är nödvändig för ett ändamål som rör Bolagets eller en tredje parts **berättigade intressen**, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter.

4.5.2 Särskilt om intresseavvägning

När behandling av personuppgifter grundar sig på Bolagets eller tredje parts berättigade intresse ska Bolaget vid varje sådan behandling göra en noggrann bedömning med ledning av nedan punkter.

- Huruvida det föreligger ett relevant förhållande mellan Bolaget och den registrerade, till exempel att den registrerade är kund hos Bolaget eller arbetar hos Bolaget.
- Huruvida den registrerade vid tidpunkten för inhämtandet av personuppgifter och i samband med inhämtandet kan förvänta sig att en behandling av dennes personuppgifter för detta ändamål kan komma att ske. Till exempel behandling av en registrerads personuppgifter i samband med att denne kontaktar Bolaget via Bolagets hemsida.
- Om personuppgifter behandlas under omständigheter där den registrerade rimligen kan förvänta sig att någon fortsatt behandling inte sker. I ett sådant fall skulle den registrerades intressen och grundläggande rättigheter komma att väga tyngre än Bolagets berättigade intresse av behandling.
- Behandling som är absolut nödvändig för Bolaget för att förhindra bedrägerier utgör ett berättigat intresse för Bolaget.
- Behandling av personuppgifter för direktmarknadsföring kan betraktas som ett berättigat intresse för Bolaget. Sådan behandling ska alltid föregås av beslut från vd i samråd med DPO.

4.5.3 Känsliga personuppgifter

Som utgångspunkt är känsliga personuppgifter förbjudna att behandla om inget undantag föreligger. Nedan undantag är de som kan vara relevanta för Bolagets verksamhet, men även andra undantag kan vara aktuella.

- Den registrerade har uttryckligen lämnat sitt samtycke till behandlingen av dessa personuppgifter för ett eller flera specifika ändamål.
- Behandlingen är nödvändig för att Bolaget ska kunna fullgöra sina skyldigheter och utöva sina särskilda rättigheter med koppling till arbetslivet. För detta krävs att det finns stöd i EU-rätt eller svensk rätt eller ett kollektivavtal som antagits med stöd av svensk rätt. *Till exempel betala ut sjuklön eller hantera anställdas tjänstepensioner och olika typer av gruppförsäkringar.*
- Behandlingen är nödvändig för att skydda den registrerades eller någon annan fysisk persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke. *Till exempel en person som blivit plötsligt sjuk och förlorat medvetandet.*
- Behandlingen rör personuppgifter som på ett tydligt sätt har offentliggjorts av den registrerade. *Till exempel att en person framträder i tv och företräder en viss politisk åsikt eller berättar om sin sjukdom.*
- Behandlingen är nödvändig för att fastställa, göra gällande eller försvara rättsliga anspråk eller som en del av domstolarnas dömande verksamhet. *Till exempel kan ett försäkringsbolag behöva samla uppgifter om en persons sjukdom, för att kunna bedöma rätten till försäkringsersättning enligt ett försäkringsavtal.*
- Behandlingen är nödvändig av hänsyn till ett viktigt allmänt intresse, på grundval av EU-rätt eller svensk rätt, vilken ska stå i proportion till det eftersträvade syftet, vara förenligt med det väsentliga innehållet i rätten till dataskydd och innehålla bestämmelser om lämpliga och särskilda åtgärder för att säkerställa den registrerades grundläggande rättigheter och intressen.
- 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 EU-rätt eller svensk rätt eller enligt avtal med yrkesverksamma på hälsoområdet och under förutsättning att relevanta villkor och skyddsåtgärder är uppfyllda. *Till exempel bedömningen av en arbetstagares arbetskapacitet.*

I Bolagets verksamhet behandlas som regel få känsliga personuppgifter. Känsliga personuppgifter kan komma att behandlas avseende Bolagets anställda, till exempel vid lönehantering och vid tecknande av försäkringar och tjänstepensioner. Bolaget kan även komma att behandla känsliga personuppgifter i samband med utförande av kundkännedomsåtgärder med avseende på till exempel bedömning av om en person är PEP (person i politiskt utsatt ställning) i enligt med lag om åtgärder mot penningtvätt och finansiering av terrorism.

I de fall Bolaget kan komma att behandla känsliga personuppgifter ska samtliga krav och rutiner följas som i den här instruktionen och i lag anges för personuppgifter. Innan behandling påbörjas ska det säkerställas att det finns ett lämpligt skydd för uppgifterna.

4.6 Konsekvensbedömning

Om en behandling av personuppgifter som kan leda till en hög risk för de registrerade ska göras måste en så kallad konsekvensbedömning avseende dataskydd utföras. Detta för att vara förutseende, förebygga risker och därmed skydda människors fri- och rättigheter. Målet är att minimera riskerna vid sådana behandlingar av personuppgifter som innebär en hög risk.

Enligt riktlinjer från den Europeiska Dataskyddsstyrelsen[1] ska, som utgångspunkt, en konsekvensbedömning göras om två eller flera av följande kriterier är uppfyllda för en viss personuppgiftsbehandling.

- Behandlingen innehåller moment av utvärdering eller profilering. Som exempel nämns banker som utför automatiserade kreditbedömningar och företag som bygger marknadsföringsprofiler baserade på Internetanvändares beteende på företagets hemsida.
- Behandlingen innefattar automatiserat beslutsfattande, exempelvis genom automatisk gallring av kandidater i en rekryteringsprocess.
- Behandlingen utgör systematisk övervakning, vilket bland annat blir aktuellt vid kameraövervakning på allmän plats.
- Behandlingen innefattar känsliga personuppgifter, där känsliga personuppgifter innefattar bland annat hälsouppgifter och biometriska- eller genetiska uppgifter, men också finansiell information och annat som är särskilt integritetskänsligt.
- Storskalig personuppgiftsbehandling. Vid bedömningen om behandlingen är storskalig tas särskild hänsyn till antalet individer som berörs, mängden personuppgifter, varaktigheten och den geografiska omfattningen.
- Behandlingen innefattar en kombination eller samkörning av personuppgiftsregister, exempelvis vid behandling av personuppgifter som är insamlade för olika syften och härrör från två eller flera källor.
- Behandling av personuppgifter som avser skyddsvärda persongrupper, dvs. där det inte råder maktbalans mellan den registrerade personen och den personuppgiftsansvarige (exempelvis i relation till anställda, barn, patienter och äldre).
- Behandling av personuppgifter på ett innovativt sätt eller med användning av ny teknik, exempelvis Internet of Things-utrustning (som kan ha stor inverkan på personers dagliga liv och integritet).
- Överföring av personuppgifter till land utanför EU.

Behandling som hindrar personer från att utöva en rättighet, använda en tjänst eller ingå ett avtal, såsom genom att nekas banklån baserad på automatisk kreditbedömning.

4.7 Särskilt om behandling av personuppgifter i e-post

Samtliga anställda ska ta del av och följa nedan information om hantering av personuppgifter vid e-posthantering. Som utgångspunkt är varje e-posthantering en behandling av personuppgifter och därmed måste lagligt stöd finnas för behandlingen.

Bolagets anställda ska följa nedan vid hantering av e-post.

[1] Europeiska dataskyddsstyrelsen är ett oberoende europeiskt organ som bidrar till en enhetlig tillämpning av dataskyddsregler i hela Europeiska unionen och främjar samarbete mellan EU:s dataskyddsmyndigheter. Dataskyddsstyrelsen består av företrädare för nationella dataskyddsmyndigheter och Europeiska datatillsynsmannen (EDPS).

- E-postmeddelande där rättslig grund för behandling saknas ska raderas omgående. Som utgångspunkt kan ett inkommande e-postmeddelande alltid hanteras i enlighet med den rättsliga grunden intresseavvägning.
- E-postmeddelande där rättslig grund för behandling finns ska efter det att behandlingen är slutförd antingen
    a) raderas, om e-postmeddelandet avser ärende där rättslig grund för fortsatt lagring inte finns, eller
    b) spara e-postmeddelandet på anvisad lagringsplats, om meddelandet avser ärende där det finns rättslig grund för fortsatt behandling (lagring). För lagring se vidare avsnitt 6.
- Utskick till flera mottagare (massutskick) ska primärt ske med e-postadresserna som ”blind copy”.
- I största möjliga mån ska enbart ett ärende per e-postmeddelande behandlas i syfte att förenkla radering, eventuell lagring och efterlevnad av krav på att på begäran ge ut registerutdrag.
- I den mån information inte behöver skickas via e-post, utan kan överföras med andra tekniska lösningar, så ska anställda använda sig av det senare alternativet.
- Vid skickande av personuppgifter ska anställda utgå från principen om uppgiftsminimering och inte skicka fler personuppgifter än vad som är nödvändigt för att uppfylla ändamålet med behandlingen och även i största möjliga mån använda sig av indirekta uppgifter, så som kundnummer och ärendenummer.
- Känsliga personuppgifter ska inte skickas i oskyddad e-post.

Vd ska säkerställa att Bolaget använder kryptering där det anses behövas, till exempel vid överföring av känsliga och integritetskänsliga uppgifter.

Bolagets anställda ska sträva efter att ha sin inkorg så tom som möjligt, med utgångspunkt att e-post ska vara en säker transportör av information, men inte en lagringsplats.

4.8 Särskilt om arbetsdator och arbetstelefon

Samtliga anställda ska använda sig av autentisering (lösenord eller liknande skydd) på sina mobiltelefoner som används i tjänsten och där behandling av personuppgifter som Bolaget är ansvarigt för förekommer. Kommunikation avseende känsliga och integritetskänsliga uppgifter ska inte skickas via sms. Gallring av sms ska ske regelbundet, helst via automatiserad inställning på telefonen och med en lagringstid på maximalt ett år. Information från sms som det finns rättslig grund för att lagra ska överföras till avsedd lagringsplats.

Datorer och mobiltelefoner tillhandahållna av Bolaget får anställd använda i begränsad omfattning för privat bruk. Kundinformation får inte lagras i personliga mappar på servern**.** I den utrustning som bolaget tillhandahåller den anställde ansvarar den enskilde anställde för hanteringen av privat information som lagras. Den anställde får inte dölja eller kryptera information i bolagets utrustning. All behandling av privat information i bolagets utrustning sker helt på den enskildes ansvar. Gällande e-post ska detta rensas minst vart femte år, dock finns mejl tillgängliga på extern server. Medarbetare ska vidta samma försiktighetsåtgärder gällande både e-post och mobiltelefoner.

5 Den registrerades rättigheter

Enligt dataskyddsförordningen har en registrerad ett antal rättigheter. Dessa rättigheter innebär att de registrerade ska få information om när och hur deras personuppgifter behandlas och ha kontroll över sina egna uppgifter. Med kontroll avses en rätt att i vissa fall få sina uppgifter rättade, raderade eller blockerade, eller att få ut eller flytta sina uppgifter.

Nedan listas den registrerades rättigheter.

- Rätt till information.
- Rätt till rättelse.
- Rätt till radering (rätten att bli glömd).
- Rätt till begränsning av behandling.
- Dataportabilitet.
- Rätt att göra invändningar.
- Råtт till att undantas från automatiserat beslutsfattande (inbegripet profilering).
- Klagomål.
- Skadestånd.

För att uppfylla kravet om den registrerades *rätt till information* har Bolaget en integritetspolicy som bland annat beskriver ändamålet med behandlingen, vilka personuppgifter som behandlas och den lagliga grunden till behandling. Bolagets kunder får genom förköpsinformationen en hänvisning till den fullständiga integritetspolicyn. Den som kontaktar Bolaget eller den som en anställd kontaktar via e-post får del av policyn genom information i e-postfot. Den som kontaktar Bolaget via hemsidan får del av policyn vid kontakten. Anställda samt befattningshavare hos Bolaget får del av integritetspolicyn vid tidpunkten för anställningen eller vid uppdatering av policyn.

För att uppfylla kravet om den registrerades *rätt till rättelse, rätt till radering, rätt till begränsning av behandling, rätt till dataportabilitet samt rätt att göra invändningar* kan en registrerad kontakta Bolaget via mail eller via kontaktformulär på hemsida.

För att uppfylla kravet om den registrerades *rätt att göra invändningar (direktmarknadsföring) samt rätt till att undantas från automatiskt beslutsfattande (inbegripet profilering)* kan en registrerad kontakta Bolaget via mail eller via kontaktformulär på hemsida. Bolaget använder sig för närvarande inte av automatiskt beslutsfattande eller profilering.

Den registrerade kan vända sig till Integritetsskyddsmyndigheten för att *rikta ett klagomål* mot Bolagets behandling av personuppgifter. Bolaget upplyser den registrerade om detta i den information den registrerade får från Bolaget.

En registrerad som lidit skada på grund av att Bolaget har behandlat dennes personuppgifter i strid med dataskyddsförordningen kan ha *rätt till skadestånd* av Bolaget eller i vissa fall det personuppgiftsbiträde som Bolaget anlitat, om biträdet brutit mot de bestämmelser som specifikt riktar sig till biträdet eller har behandlat uppgifter i strid med Bolagets instruktioner. Den registrerade kan rikta en sådan begäran till Bolaget via kontaktformulär på hemsida eller brev, alternativt väcka skadeståndstalan i domstol.

En anställd kan kontakta vd eller DPO för att utöva sina rättigheter enligt ovan. Övriga registrerade kan utöva sina rättigheter via kontaktformulär på Bolagets hemsida eller kontakt via brev.

6 Spara och lagra personuppgifter

6.1 Inledning

Dokument innehållandes personuppgifter ska sparas med utgångspunkt i den lagringsplats som är angiven i personuppgiftsregistret. Nedan följer instruktioner för enskilda kategorier av personuppgifter. Lagringen ska även omfattas av rutiner för gallring så att information som inte behöver lagras under en längre period, exempelvis för att efterleva andra regelverk, raderas regelbundet. Gallringsrutiner ska anges i personuppgiftsregistret.

6.2 Kunddokumentation och försäkringshandlingar

Kundärenden, oavsett kommunikationsmedel och typ av dokument, ska alltid lagras på kundkortet i Bolagets CRM-system. Anställd får inte spara några dokument innehållandes personuppgifter på egen dator eller på annan plats än i CRM, om det inte är för tillfällig behandling. Uppgifterna ska efter att en sådan tillfällig behandling är slutförd raderas från den anställdas dator.

I kommunikationen mellan anknutna ombud och Bolaget ska meddelandefunktionen i systemet BrokerWeb användas. I kommunikationen mellan slutkund och Bolaget ska meddelandefunktionen i systemet SVP Online användas.

6.3 Samarbetspartners och leverantörer

Kommunikation och korrespondens med en samarbetspartner till Bolaget som finns behov av att lagra ska sparas tillsammans med annan sådan kommunikation och korrespondens på dedikerad plats på server hos Aderian som är leverantör av IT-tjänster.

6.4 Manuellt eller automatiskt skapade listor

I den mån register eller listor skapas, antingen manuellt eller automatiskt, ska följande iakttas.

1. Använd endast den information och de fält som är nödvändiga för det ändamål du ska behandla personuppgifterna.
2. Om behandlingen inte är tillfällig ska lagringen noteras i personuppgiftsregistret.
3. Informationen/listan ska raderas efter det att behandlingen är slutförd.

6.5 Gallring

Personuppgifter får inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Personuppgifter ska gallras ur Bolagets register när uppgifterna inte längre behövs. Det innebär att anställda ska undvika att slentrianmässigt bevara personuppgifter under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen.

Detaljerade instruktioner kring rensning av personuppgifter framgår av personuppgiftsregistret samt eventuell särskild rutinbeskrivning.

7 Personuppgiftsbiträde

7.1 Bolagets anlitande av personuppgiftsbiträden

I de fall ett personuppgiftsbiträde anlitas ska Bolaget inhämta tillräckliga garantier från biträdet om att biträdet har eller kommer att genomföra lämpliga organisatoriska och tekniska åtgärder så att

behandlingen som biträdet utför uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

Den behandling av uppgifter som personuppgiftbiträdet utför för Bolagets räkning ska regleras i ett avtal i enlighet med artikel 28 i dataskyddsförordningen. Samtliga biträden som Bolaget använder och har ingått avtal med ska antecknas i Bolagets register över personuppgiftsbiträden.

Om en uppdragstagare agerar som personuppgiftsbiträde eller inte ska avgöras i varje enskilt fall i enlighet med vägledning från IMY och Dataskyddsstyrelsen.

7.2 Bolagets agerande som personuppgiftsbiträde

I de fall Bolaget ingår avtal om att agera som ett personuppgiftsbiträde ska detta antecknas i Bolagets register över personuppgiftsbiträden.

8 IT-verksamhet

8.1 Ansvar

Bolagets vd ansvarar för att följande instruktioner för IT-verksamheten efterlevs.

8.2 Upphandling och utveckling av IT-lösningar

För all upphandling och utveckling av IT-lösningar ska hänsyn tas till den personliga integriteten för den information som systemen ska behandla. För att efterleva principerna inbyggt dataskydd och dataskydd som standard, som uttryckligen nämns i dataskyddsförordningen, ska Bolaget utgå från nedan.

1. Ta hänsyn till integritetsaspekten i hela livscykeln genom att
    a) inte samla in mer information än vad som behövs,
    b) inte lagra informationen längre än vad som behövs, och
    c) inte använda informationen till annat än vad den samlades in för.

2. Fastställ och utgå från ändamålet för behandlingen.
    a) Ändamålet för behandlingen (insamling och övrig hantering) ska bestämmas i förväg.
    b) Fastställ vilka personuppgifter som krävs för att tillgodose ändamålet.
    c) Kraven på systemet och processer måste utgå från ändamålet, och med målet att minska integritetsriskerna, exempelvis genom att
        - begränsa användandet till uppgifter som enbart indirekt pekar ut en registrerad,
        - begränsa användandet till uppgifter som är mindre känsliga,
        - ersätta namn med exempelvis pseudonymer,
        - inte rutinmässigt använda personnummer som fält i databaser, och
        - anonymisera information där personuppgifter inte är nödvändiga.

3. Begränsa åtkomsten till uppgifterna.
    a) Endast anställd som har behov av uppgifterna för att utföra sin arbetsuppgift ska ha behörighet att se och behandla uppgifterna.

4. Skydda uppgifterna.
    a) IT-system som exponeras mot internet måste ha ett större mått av säkerhet.
    b) Ju känsligare uppgifter desto högre säkerhet.
        a. Utöver behörighetsstyrning bör det exempelvis finnas
            - funktioner för autentisering (minst lösenord) och
            - möjlighet att använda kryptering vid a) kommunikation över internet, b) i databaser och c) på mobila enheter.
    c) Rutiner för och tydlig information om säkerhet till systemets användare.
    d) En logg som kan användas till att utreda obehörig åtkomst till personuppgifter.
    e) Stöd för säkerhetskopiering, med säkerställande att kopiorna inte sparas för länge (som regel inte längre än 30 dagar).
    f) Säker radering, d.v.s. skydd mot att data läcker efter att hela eller delar av ett system tagits ur drift.
    g) Observera att loggar och säkerhetskopior kan innehålla personuppgifter och att integritetsrisken omfattar även dessa.

5. Formulera tydliga krav till Bolagets leverantörer av IT-stöd.

9 Dataskyddsombud – DPO

DPO är den som är kontaktperson för Bolagets kunder om de exempelvis vill få veta vilka uppgifter som finns registrerade om dem.

Bolagets vd är DPO. Kontaktuppgift: info@svp.se. Bolaget ska till IMY anmäla den som är utsedd att vara Bolagets DPO.

DPO:s arbetsuppgifter är främst att

- samla in information om hur Bolaget behandlar personuppgifter,
- kontrollera att Bolaget följer bestämmelser och interna styrdokument,
- informera och ge råd inom Bolaget,
- ge råd om konsekvensbedömningar,
- vara kontaktperson gentemot IMY,
- vara kontaktperson för de registrerade och personalen inom Bolaget, samt
- samarbeta med IMY, t ex vid inspektioner.

10 Personuppgiftsincidenter

10.1 Beskrivning och internt system för rapportering

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Exempel på incidenter är

- diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning,
- finansiell förlust,
- brott mot sekretess eller tystnadsplikt.

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har

- blivit förstörda
- gått förlorade på annat sätt, eller
- kommit i orätta händer.

Det spelar ingen roll om det har skett oavsiktligt eller avsiktligt. Båda fallen utgör personuppgiftsincidenter.

Samtliga anställda ska rapportera incidenter i enlighet med Bolagets interna regler om hantering av incidenter. Samtliga dessa incidenter noteras sedan särskilt i Bolagets register över personuppgiftsincidenter. Vid osäkerhet om rapportering ska ske ska du som anställd iaktta en försiktighetsprincip och ändå göra en rapport.

10.2 Handlingsplan vid inträffande

10.2.1 Ansvarig för genomförande

DPO är ansvarig för att samtliga steg i handlingsplanen vidtas.

10.2.2 Bedöm riskerna för personer som drabbats av personuppgiftsincident

Vid inträffande av en personuppgiftsincident ska Bolaget omedelbart bedöma både konsekvensen (allvarligheten) av den potentiella eller faktiska påverkan incidenten kan ha och sannolikheten för att detta inträffar. Det är risken för människors friheter och rättigheter som ska bedömas.

- Hur allvarliga kan konsekvenserna bli?
- Hur sannolikt är det att enskilda personer drabbas?

Om personuppgiftsincidenten är allvarlig är risken högre. Om sannolikheten för konsekvenser är stor är risken också högre.

10.2.3 Anmälan till Integritetsskyddsmyndigheten

Om det är troligt att personuppgiftsincidenten kommer att medföra en risk för de registrerade har Bolaget en skyldighet att meddela IMY. Om det är osannolikt att en personuppgiftsincident medför risker behöver Bolaget inte meddela IMY.

Personuppgiftsincidenten ska anmälas till IMY inom 72 timmar efter det att överträdelsen har upptäckts. Bolaget ska innan anmälan ske samla in så mycket information som möjligt om den inträffade incidenten.

Om Bolaget inte har möjlighet att utreda eller skaffa sig all information inom 72 timmar kan Bolaget komplettera anmälan inom 2 veckor efter det att anmälan inkommit till IMY. Är incidenten allvarligt ska Bolaget prioritera att anmäla incidenten till IMY så fort som möjligt, trots att Bolaget inte har all information.

Om en incident inträffar hos ett personuppgiftsbiträde till Bolaget måste biträdet omedelbart rapportera det till Bolaget. Det är dock Bolaget som är ansvarigt att i förekommande fall anmäla incidenten till IMY.

10.2.4 Informera de registrerade

Enligt dataskyddsförordningen måste Bolaget informera de registrerade direkt och utan onödigt dröjsmål om en personuppgiftsincident sannolikt leder till en hög risk för fysiska personers rättigheter och friheter.

Om risken bedöms som hög ska Bolaget omedelbart informera de registrerade, särskilt om det finns behov av att mildra en omedelbar risk för skador. Bolaget ska om möjligt hjälpa de registrerade att vidta åtgärder för att skydda sig mot effekterna av en personuppgiftsincident.

I informationen till de registrerade ska minst nedan finnas med.

- En klar och tydlig beskrivning av orsaken till personuppgiftsincidenten.
- Namn och kontaktuppgifter till den som är ansvarig för dataskyddsfrågor hos Bolaget.
- En beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten.
- En beskrivning över vad Bolaget har gjort, eller tänker göra, för att hantera personuppgiftsincidenten.
- I förkommande fall en beskrivning av vad Bolaget har gjort för att mildra eventuella negativa effekter.

10.2.5 Dokumentera

Bolaget ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för Integritetsskyddsmyndigheten att kontrollera efterlevnaden av Bolagets anmälningsskyldighet samt ytterligare skyldigheter som följer av anmälan om personuppgiftsincident.

Samtliga incidenter ska dokumenteras, även dem som inte lett till en rapportering till IMY.

11 Fastställande och revidering

DPO ska ansvara för innehållet i denna instruktion. Instruktionen ska fastställas av styrelsen vid behov eller minst årligen.