# Dataskyddspolicy

Senast fastställd 2023-04-19
av styrelsen i Investerum AB

# Innehåll

# 1 Inledning

## 1.1 Bakgrund och syfte

Styrelsen i Investerum AB (”**Investerum**” eller ”**Bolaget**”) har, mot bakgrund av dataskyddsregelverket fastställt följande policy för sitt arbete med dataskydd och personuppgiftshantering. Dataskyddspolicyn fastställer övergripande principer och riktlinjer för Investerums verksamhet avseende adekvat dataskydd och regelefterlevnad rörande personuppgiftsbehandling.

Dataskyddspolicyn syftar även till att främja enskildas personers kontroll och rättigheter rörande sina personuppgifter, när dessa behandlas av Investerum. Bestämmelserna i Dataskyddspolicyn syftar också till att säkerställa kunders och andra enskilda personers rätt att ha insyn i och kontroll över de personuppgifter som behandlas av Investerum.

## 1.2 Dataskyddspolicyns tillämpningsområde

Dataskyddspolicyn är tillämplig på alla delar av Investerums verksamhet, även verksamhet som har outsourcats och ska tillämpas av styrelseledamöter, ledning, samtliga anställda och uppdragstagare som på något sätt berörs av Investerums personuppgiftshantering.

Dataskyddspolicyn omfattar samtliga personuppgifter som hanteras inom ramen för Investerums verksamhet, oavsett om de behandlas strukturerat eller inte.

# 2 Organisation och ansvar

## 2.1 Styrelsen

Investerums styrelse är ytterst ansvarig för att Bolaget följer dataskyddsregelverket i verksamheten.

Styrelsen ansvarar för att fastställa denna policy minst en gång per år.

## 2.2 VD

Bolagets VD ansvarar övergripande för att införa processer och mekanismer för att upprätthålla regelefterlevnaden utifrån styrelsens direktiv och ska säkerställa att Dataskyddspolicyn implementeras och upprätthålls i verksamheten.

## 2.3 IT-ansvarig

Bolagets IT-ansvarig ansvarar för den dagliga driften och tillgången till Bolagets system, lösenord för datorer, företagsmobiler osv.

Detta omfattar bland annat att ansvara för:

- Administratörsrättigheter i system och infrastruktur
- Tilldela access till personuppgifter
- Begränsa access till personuppgifter
- Att företagskopplad hårdvara har relevant brandvägg och antivirussystem

IT-ansvarig har ansvar över den delen som berör frågor gällande bolagets digitala infrastruktur. I förhållande till dataskydd och personuppgiftsbehandling ansvarar IT-ansvarig för att:

- Förteckning över Bolagets personuppgiftsbehandling hålls uppdaterat, se Bilaga 1.
- I första försvarslinjen vid behov utföra kontroller och fungera som löpande stöd i verksamheten avseende personuppgiftshantering.
- Personuppgifter hanteras på ett ansvarfullt sätt inom IT-organisationen.
- Hålla en hög nivå av säkerhet inom teknikutveckling och drift.
- Se till att utvecklarna använder ”privacy by design” i olika processer.
- Skapa förutsättningar för Bolaget att hålla sig uppdaterad med bäst praxis för säker kodning, utveckling inom IT-säkerhet och test.
- Informera VD och Funktionen för regelefterlevnad om säkerhetsbuggar och intrång som är relaterade till personuppgiftsincidenter.

## 2.4 Kontrollfunktion

Funktionen för regelefterlevnad ansvarar för att i andra försvarslinjen från tid till annan utföra oberoende kontroller av Bolagets efterlevnad av dataskyddsregelverket och Dataskyddspolicyn.

Därtill skall funktionen fungera som löpande stöd i verksamheten avseende personuppgiftshantering, bevaka praxis samt även kunna ge råd vid frågor eller oklarheter som uppkommer med anledning av innehållet i denna policy.

## 2.5 Avdelningschef/Ansvarig

Ansvarar för att det upprättas ett underliggande dokument till detta styrdokument som tydliggör rutiner kopplat till medarbetarnas arbetssätt avseende hantering av personuppgifter i den dagliga verksamheten. VD ska sedan godkänna sådana rutiner. Se vidare i bilaga.

## 2.6 Systemägare

För varje IT-system som Investerum har finns det en utsedd systemägare. Systemägaren ansvarar för att tekniska och manuella rutiner för personuppgiftshantering i respektive system följer kraven i Dataskyddspolicyn. Systemägare framgår av bilaga.

### 2.7 Medarbetare

Samtliga medarbetare vid Investerum skall genomgå internutbildning rörande personuppgiftsbehandling samt ha grundläggande kunskaper om dataskyddsregelverket och aktuell praxis. Vidare följer även ett ansvar att följa de riktlinjer och rutiner som har satts upp genom Dataskyddspolicyn.

### 2.8 Definitioner

*Behandling av personuppgifter*: med behandling menas en åtgärd eller en kombination av åtgärder som vidtas avseende personuppgifter, vare sig det sker med hjälp av en dator eller manuellt, automatiserat eller inte. Exempel på behandling av personuppgifter är: insamling, registrering, lagring, överföring, bearbetning.

Dataskyddsförordningen (GDPR): EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av 2018:218 den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän dataskyddsförordning)

*Dataskyddsregelverket:* Dataskyddsförordningen och Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning och där tillhörande nationell reglering såsom lagar, föreskrifter, allmänna råd och praxis.

*Gallring*: gallring av personuppgifter innebär radering av personuppgiften eller att personuppgiften anonymiseras på sådant sätt att den inte längre ensamt eller i kombination med andra uppgifter innebär att en fysisk person kan identifieras till uppgiften eller i övrigt kopplas samman med uppgiften.

*Lagring*: lagring innebär att personuppgiften sparas digitalt eller fysiskt.

*Personuppgift*: all slags information som direkt eller indirekt kan hänföras till en fysisk person i livet. Personuppgifter förekommer både i bolagets direkta affärsverksamhet (exempelvis beträffade kunder) och i den del av verksamheten som avser Bolagets anställda och uppdragstagare.

*Personuppgiftsincident:* en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

*Registrerad*: den fysiska person som personuppgiften/-uppgifterna avser. För Bolagets räkning avser det främst kunder och anställda.

*Särskilda kategorier av personuppgifter*: personuppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening samt genetiska och biometriska uppgifter, uppgifter om hälsa, sexualliv eller sexuell läggning (tidigare kallat ”känsliga personuppgifter”).

## 3 Dataskyddsregelverket, legalt

### 3.1 Laglig grund för behandlingen

För att en behandling av personuppgifter ska vara förenlig med Dataskyddsregelverket krävs det att behandlingen baseras på laglig grund.

Dataskyddslagregelverket listar nedan sex grunder som måste gälla för att personuppgiftsbehandling skall vara tillåtet;

1) Den registrerade har lämnat sitt **samtycke** till personuppgiftsbehandlingen,
2) för att den personuppgiftsansvarige skall kunna fullgöra en **rättslig förpliktelse** som åvilar denne;
3) behandlingen är nödvändig för att **fullgöra ett avtal** som den registrerade är part av.
4) för att **skydda intressen som är av grundläggande betydelse** för den registrerade.
5) att behandlingen är nödvändig för att utföra en uppgift av **allmänt intresse**.
6) den personuppgiftsansvarige har ett **berättigat intresse** för behandlingen.

Investerum behandlar bara personuppgifter utifrån laglig grund; se bilaga registerförteckning.

### 3.1.1 Särskilda kategorier av personuppgifter

Särskilda kategorier av personuppgifter, även kallade känsliga personuppgifter, är uppgifter om ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening, genetiska och biometriska data och uppgifter om hälsa samt sexualliv eller sexuell läggning. Dessa är förbjudna att behandla om behandlingen inte faller under ett av nedan angivna undantag;

- Uttryckligt samtycke från den registrerade.
- Den personuppgiftsansvariges rättsliga skyldighet inom arbetsrätten och områden som sociala trygghet och socialt skydd.
- Skydd för den registrerades eller någon annan annans persons grundläggande intressen när den registrerade är fysiskt eller rättsligt förhindrad att ge sitt samtycke.
- Vid den registrerades eget offentliggörande.
- Vid rättsligt anspråk.
- Vid en arbetsuppgift av allmänt intresse.
- Inom hälso- och sjukvård.
- Vid allmänt intresse på folkhälsoområdet.
- För arkivering samt historiska, vetenskapliga och statistiska ändamål.

Investerum bedömer att behandling av så kallade känsliga personuppgifter faller under någon av undantagen som finns listade. Till exempel i rollen som försäkringsförmedlare kan det krävas att Bolaget samlar in information om den registrerades hälsotillstånd för att ha möjlighet att utföra sitt uppdrag som försäkringsförmedlare.

## 3.2 Investerums personuppgiftsbehandling

Investerum behandlar personuppgifter för i huvudsak tre kategorier av registrerade;

- Kunder – inbegripet kunder som är fysiska personer samt även företrädare för eller kontaktpersoner hos de enskilda näringsidkare och juridiska personer med vilka Bolaget har ett avtalsförhållande,
- Medarbetare och Uppdragstagare, samt
- Övriga – inbegripet bland annat personer som uttryckligen visat intresse för Investerums tjänster, såsom tex eventuella blivande kunder, personer som har förekommit i Investerums HR-process vid eventuella rekryteringar, referenser till nyrekryteringar.

Personuppgifter som Investerum behandlar kan kategoriseras enligt följande:

- Identifieringsuppgifter: exempelvis namn och personnummer
- Kontaktuppgifter: exempelvis adresser och telefonnummer
- Ekonomisk information: exempelvis transaktionsinformation

- Uppgifter som krävs enligt lag: exempelvis uppgift om skattehemvist eller utländskt skatteregistreringsnummer, uppgifter som krävs för bekämpning av penningtvätt och kundkännedom
- Särskilda kategorier av personuppgifter: exempelvis vissa uppgifter om medarbetare

Investerum omfattas inte av lagkrav på en registerförteckning då Bolaget har färre än 250 anställda. Bolaget har dock gjort en övergripande kartläggning av ovan nämnda personuppgiftsbehandling i enlighet med kraven i artikel 30 i GDPR, se förteckning i Bilaga 1.

# 4 Grundläggande principer för dataskydd

Det personliga integritetsskyddet är en grundpelare i Dataskyddsregelverket vilket innebär att integritetsskyddet ska iakttas genom hela livscykeln av personuppgiftsbehandlingen. Andra grundläggande principer som Bolaget skall följa vid personuppgiftsbehandling är principerna om insamling, uppgiftsminimering, korrekthet, lagring och integritet.

Att en behandling ska vara *laglig och korrekt* betyder att den inte får strida mot andra bestämmelser i dataskyddsförordningen, framförallt att det ska finnas en laglig grund. Vidare ska behandlingen vara öppen och transparant gentemot den registrerade.

*Korrekthet* innebär också att personuppgifterna ska vara korrekta och uppdaterad. Den personuppgiftsansvariga och/eller personuppgiftbiträden/underbiträden har skyldigheten att säkerställa att personuppgifter som är felaktiga ska raderas eller rättas utan dröjsmål.

Vid behandling av personuppgifter ska uppgifter enbart samlas in för särskilda, uttryckligt angivna och berättigade ändamål. I praktiken innebär detta att den som samlar in personuppgifterna inte senare får behandla personuppgifterna för ett *annat* ändamål (s.k. *ändamålsbegränsning*).

Vid inhämtande av personuppgifter krävs det att enbart det uppgifter som är adekvata, relevanta och inte för omfattande för ändamålet inhämtats. Det betyder alltså att det inte är tillåtet att inhämta uppgifter för obestämda framtida behov eller fler än vad behovet kräver (s.k. *uppgiftsminimering*).

I enlighet med Dataskyddsregelverket ska Investerum inte spara fler uppgifter än nödvändigt eller under längre tid än nödvändigt. Vidare är målet att ge ramarna för att säkerställa att gallring av personuppgifter sker på ett ändamålsenligt och effektivt sätt samt i enlighet med externa regler (s.k. *lagringsminimering*). För närmare vägledning hänvisas till Bilaga 1 Registerförteckning (innehållande Gallringstabell) och Bilaga 2, Vägledning rörande gallring av personuppgifter.

De personuppgifter som har inhämtats ska skyddas gentemot förlust, förstöring eller skada genom olyckshändelse. Obehörig eller otillåten behandling ska också ingå i skyddsåtgärderna.

Det är den som behandlar personuppgifterna, personuppgiftsansvariga och/eller personuppgiftsbiträden/underbiträden, som ansvarar för att dessa principer efterlevs och efterföljs.

# 5 Interna regler för Investerums personuppgiftshantering

## 5.1 Förteckning över personuppgiftsbehandling

Investerum för en registerförteckning över personuppgifts-behandlingen i verksamheten, se bilaga. Registerförteckningen syftar till att skapa intern kontroll över personuppgiftshanteringen samt är ett led i att kunna uppvisa efterlevnad av Dataskyddsregelverket.

Registerförteckningen förvaltas av samt hålls löpande uppdaterad av rollen för ”First line of Defence”. Inbyggt dataskydd (”Privacy by design”) och IT

De huvudsakliga system anställda har tillgång till efter behov är följande:

1. *Microsoft Dynamics: CRM*
   Kundhanteringssystem
   Alla i organisationen har behörighet till den kundinformation som finns i CRM.
   Tillgången fyller olika syften beroende på vilken roll en anställd innehar.

2. *Secura*
   Transaktionssystem
   Begränsad tillgång, dvs de som jobbar med rådgivning eller administration samt IT-ansvarig.
   Syftet med tillgång är kundhantering, bokföring och uppgifter gällande bolagets finansiella instrument.

3. *CM1-systemet*
   Verktyg för att utföra kundkännedom
   Begränsad tillgång. Endast administrativ personal, IT-ansvarig och IRC har tillgång till systemet.
   Syftet med tillgången till systemet är för att admin-personal ska utföra kundkännedom kopplat till penningtvätt.

## 1) Inbyggt dataskydd och IT

Investerum måste ha ett adekvat skydd för de personuppgifter som behandlas i verksamheten.

Kraven i dataskyddsregelverket gällande Inbyggt Dataskydd (på engelska den numera väletablerade termen *”Privacy by design”*) innebär att Investerum ska genomföra lämpliga tekniska och organisatoriska åtgärder för att skydda den personliga integriteten. Mängden personuppgifter som samlas in skall minimeras, åtkomsten till uppgifterna ska kunna begränsas och uppgifternas skall kunna skyddas genom upprättande ett användarvänligt IT-system.

För att kunna leva upp till kravet på Inbyggt Dataskydd har Investerum gjort en kartläggning över vilka personuppgifter som behandlas i respektive IT-system, vilken bidrar till att upprätta och uppdatera förteckningen över vilka personuppgifter som behandlas och i vilket syfte.

För att skydda personuppgifter och begränsa åtkomst till dessa krävs det att systembehörigheter är begränsade till enbart de medarbetare som har behörighet att utföra arbetsuppgifter som berörs av personuppgiftshantering. Se vidare nedan avsnitt 5.3.2 om Behörighetsstyrning.

Kartläggningen av personuppgiftsbehandling av personuppgifter i IT-system framgår av registerförteckningen i Bilaga 1.

## 2) Behörighetsstyrning

Investerum har en behörighetsstyrning avseende IT-miljön som syftar till att skapa skydd för de personuppgifter som hanteras i verksamheten. Utgångspunkten för Investerums behörighetsstyrning är behovsstyrt, dvs. enbart den funktion/roll som måste ha tillgång till uppgifterna inom ramen för det arbete denna funktion/roll utför ska ha tillgång till uppgifterna.  Behörighet ska beställas och beslutas av respektive chef och ska utföras och uppdateras av Bolagets IT-ansvarig.

## 5.2 Lagring och gallring

### 5.2.1 Allmänt om lagring och gallring

I enlighet med Dataskyddsregelverket och de grundläggande principerna för behandling av personuppgifter ska personuppgifter enbart behandlas och lagras för de ändamål som de ursprungligen inhämtades för, s.k. *uppgiftsminimering.* Personuppgifter ska inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen, s.k. *lagringsminimering.*

Om ändamålet inte längre är giltigt skall uppgifterna enligt huvudregeln i Dataskyddsförordningen raderas ”utan onödigt dröjsmål”.

### 5.2.2 Gallring av personuppgifter i verksamheten

Personuppgifter i Investerums verksamhet ska gallras när den lagliga grunden för behandling upphör samt med beaktande av eventuell särreglering i speciallagstiftning.

Dataskyddsprinciper, externa regelverkskrav samt registrerades rättigheter ska vara utgångspunkt för att avgöra lagringstider och gallringsrutiner för de personuppgifter som Investerum behandlar.

Se Bilaga 1 och Bilaga 2 för närmare vägledning rörande gallring av personuppgifter.

## 5.3 Ostrukturerat material

### 5.3.1 Allmänt om personuppgifter i ostrukturerat material

Tidigare personuppgiftsreglering i Personuppgiftslagen (PUL) omfattade inte personuppgiftshantering i ostrukturerat material, dvs. sådan behandling undantogs regelverket genom den s.k. *missbruksregeln.* I nuvarande dataskyddslagstiftning görs ingen skillnad på personuppgiftsbehandling som sker strukturerat eller ostrukturerat, vilket innebär att dataskyddslagsregelverket ska tillämpas lika på båda dessa sorters personuppgiftsbehandling. Det sagda innebär att samtliga regler i Dataskyddspolicyn rörande exempelvis lagring, gallring, skydd för personuppgifter och registrerades rättigheter gäller även för personuppgifter i ostrukturerat material.

### 5.3.2 Bolagets personuppgiftshantering i ostrukturerat material

Bolaget har viss personuppgiftshantering i ostrukturerat material, exempelvis:

- Uppgifter i mejl samt digitala och fysiska dokument, såsom i:
  - HR-processen gällande rekrytering av personal: sparas i ”molnet”
  - HR-processen gällande anställda; där information sparas i ”molnet” och i fysiska pärmar
  - HR-processen gällande sjukintyg från anställda: sparas fysiskt i personalakter i pärmar på HR-ansvarigs rum.
  - HR-processen gällande medarbetarsamtal: dokumenteras i anteckningsblock och sparas fysiskt i personalakten.
  - Kundprocessen gällande personuppgifter rörande kunder och anhöriga förvaras i pärmar och i mappar på dator.

- Personuppgifter på lokala enheter samt i digitala filer och mappar på servern.

## 5.4 Information till registrerad

Dataskyddsregelverket ställer krav på att viss information måste lämnas till den registrerade vid inhämtandet av personuppgifter.

Vidare ställs det olika krav på *när* informationen ska lämnas till den registrerade beroende på hur den har inhämtats. I det fall informationen har inhämtats från den registrerade ska ovanstående information lämnas vid insamlingstillfället. Om informationen inte har inhämtats från den registrerade ska informationen senast lämnas en månad efter inhämtandet. Har informationen inhämtats med ändamål för kommunikation med den registrerade ska informationen lämnas vid första kommunikationstillfället. Om personuppgifterna ska användas för utlämnande till annan mottagare, ska informationen lämnas ut första gången utlämningen sker.

Se Bilaga 4 för vilken typ av information som måste lämnas när personuppgifterna har inhämtats respektive inte har inhämtats från den registrerade.

### 5.4.1 Undantag från när information måste ges

När information har inhämtats från den registrerade men den registrerade redan besitter informationen krävs det inte att den personuppgiftsansvariga lämnar informationen igen.

När informationen inte har inhämtats från den registrerade krävs det inte att information lämnas till den registrerade i följande fall:

- om den registrerade redan har informationen
- om tillhandahållandet av informationen visar sig vara en oproportionell börda
- om ändamålet med behandlingen blir omöjligt att utföra i och med utlämnandet
- om det finns lagligt stöd för att inte lämna ut uppgifterna
- om det finns lagstadgade sekretessförpliktelser som omöjliggör utlämnandet av informationen.

### 5.4.2 Bolagets informationsgivning

Investerum ska i alla situationer tillgängliggöra, men även i vissa fall tillhandahålla information om hur verksamheten behandlar registrerades personuppgifter samt villkoren för utövandet av den registrerades rättigheter.

Informationen ska vara skriftlig och finnas tillgänglig på ett sådant sätt att samtliga registrerade kan ta del av informationen. Vidare ska informationen vara utformad på ett enkelt och tydligt sätt samt i ett lätt tillgängligt format.

Investerum har tillgängliggjort informationen på sin webbplats samt även som en del av de allmänna villkor som samtliga av Bolagets kunder får del av när en avtalsrelation etableras.

Dataskyddsregelverket innefattar flertalet bestämmelser som syftar till att ge registrerade kontroll över hur dennes personuppgifter hanteras samt möjlighet att utöva vissa rättigheter kopplade till sin personuppgiftshantering. Dessa rättigheter innefattar rätt till registerutdrag, rätt till rättelse, rätt till radering (s.k. ”rätten att bli glömd”) och rätt till dataportabilitet.

Investerum ska underlätta utövandet av den registrerades rättigheter. Vidare ska Investerum utan onödigt dröjsmål och senast en månad efter att ha mottagit begäran tillhandahålla den registrerade information om de åtgärder som vidtagits med anledning av begäran. Information och åtgärder ska tillhandahållas kostnadsfritt så länge den registrerades begäran inte är uppenbart ogrundade eller orimliga, särskilt beaktat

att begäran skulle vara tätt återkommande. I dessa fall får Investerum ta ut en rimlig avgift för att täcka administrativa kostnader.

### 5.4.3 Rätten till registerutdrag

GDPR ställer krav på att bolag måste lämna ut viss information gällande de personuppgifter som bolaget behandlar den registrerade eller anställd.

I enlighet med artikel 15 ska den registrerade ha rätt till att få tillgång till sin information i form av ett registerdrag i elektronisk form eller i fysisk form som skickas via post. Vid elektroniskt registerutdrag ska utdraget skickas som en krypterad PDF-fil och ett lösenord ska skickas via sms till den registrerade. I regel har en organisation en månad på sig att lämna ut registerutdraget till den registrerade.

I det fall begäran om registerutdrag anses vara orimlig och/eller ogrundad, exempelvis om den registrerade återkommer med begäran om registerutdrag gång på gång, har en organisation rätt att ta ut en administrativ avgift samt kan också i sådana fall ha rätt att vägra lämna ut ett registerutdrag till den registrerade.

Förutom en kopia av personuppgifterna ska ett registerutdrag till den registrerade, i enlighet med artikel 30, innehålla följande information:

- Ändamålet/ändamålen med behandlingen av personuppgifter.
- Vilka kategorier av personuppgifter som behandlas.
- Mottagare eller kategorier av mottagare av personuppgifterna, vilka som finns i tredjeland eller är internationella organisationer (detta innefattar IT-leverantörer) och vilka lämpliga skyddsåtgärder som vidtagits vid eventuell överföring till tredjeland/internationell organisation.
- Under hur lång tid personuppgifterna kommer att bevaras, eller då det är svårt att lämna exakt tidsangivelse vad som krävs för att personuppgifterna ska gallras.
- Information om vilka rättigheter den registrerade har (rätten att bli glömd, rättelse, dataportabilitet etc.)
- Rätten att lämna klagomål till Integritetsskyddsmyndigheten
- Varifrån personuppgifterna har hämtats om de inte har hämtats från den registrerade själv.
- Förekomsten av automatiserat beslutsfattande, exempelvis profilering, och i sådana fall lämna en förklaring till varför automatiserat beslutfattande sker och vilka följder ett sådant beslutsfattande kan få.

Det är viktigt vid utlämnade av registerutdrag att sådant utdrag inte får en negativ inverkan på andras integritet. I praktiken innebär det exempelvis att Investerum ska stryka över eventuell information om tredjeperson i det fall de förekommer i registerutdraget.

Investerum har upprättat en separat rutin för begäran av registerutdrag, se begäran om registerutdrag.

För mer information om hur Investerum hanterar begäran om registerutdrag, se Rutin för hantering av kunders GDPR-begäran.

### 5.4.4 Rätt till rättelse

Artikel 16 GDPR ger den registrerades rätt till rättelse innebär att Bolaget vid en begäran från en registrerad utan onödigt dröjsmål ska rätta felaktiga personuppgifter om den registrerade.

Den registrerade har möjlighet att inkomma med en begäran om rättelse via Bolagets hemsida www.investerum.se/gdpr. Bolaget har efter inkommen begäran 30 dagar på sig att utföra rättelsen och återkomma till den registrerade med en bekräfta att ärendet har hanterats.

För mer information om hur Investerum hanterar begäran om rättelse, se Rutin för hantering av kunders GDPR-begäran.

### 5.4.5 Dataportabilitet

Dataportabilitet innebär att den registrerade ska ha rätt att få ut de personuppgifter som rör honom eller henne och som han eller hon har tillhandahållit Bolaget i ett strukturerat, allmänt använt och maskinläsbart format och ha rätt att överföra dessa uppgifter till en annan personuppgiftsansvarig utan att Bolaget hindrar detta.

Rätten till dataportabilitet gäller endast personuppgifter där behandlingen grundar sig på samtycke eller på ett avtal. Bolaget påbörjar under 2020 implementering av lämpliga tekniska lösningar för att möjliggöra dataportabilitet samt effektivt kunna tillmötesgå en kunds efterfrågan om dataportabilitet.

### 5.4.6 Rätten att bli glömd

Artikel 17 i Dataskyddsregelverket innefattar en rätt för den registrerade att bli bortglömd (”rätt att bli raderad”). Med andra ord har den registrerade rätten att få alla sina personuppgifter raderade i följande fall:

- om ändamålet med behandlingen för varför personuppgifterna inhämtats har upphört,
- om behandlingen grundar sig på den registrerades samtycke och den registrerade återkallar sitt samtycke,
- om behandlingens ändamål baseras på direktmarknadsföring,
- om behandlingen av den registrerades personuppgifter saknar lagliggrund eller radering av personuppgifter krävs för att uppfylla en rättslig skyldighet.

Vidare krävs det i det fall där den registrerades personuppgifter har lämnats ut till tredje part och den registrerade kräver radering att även den tredje parten blir informerad om raderingen.[1]

På grund av att Investerum är ett värdepappersbolag har Bolaget en skyldighet till att behålla en stor del av de personuppgifter som samlas in om den registrerade. Speciell hänsyn tas till *Bokföringslagen* (information ska behållas i upp till sju år) och *Preskriptionslagen* (information kan komma att behållas i upp till 10 år). Gränsen för hur länge Bolaget får behålla personuppgifter om en kund *efter att de har slutat att vara kund* är idag 10 år. När 10 års-gränsen har passerats ska alla personuppgifter som rör den registrerade raderas från Bolagets system.

[1] Det finns undantag till denna skyldighet, om det skulle anse sig vara omöjligt att kontakta tredje part eller innebära en alltför betungande insats.

Den registrerade har möjlighet att inkomma med en begäran om radering via Bolagets hemsida www.investerum.se/gdpr. Bolaget har efter inkommen begäran 30 dagar på sig att utföra rättelsen och återkomma till den registrerade med en bekräfta att ärendet har hanterats.

För mer information om hur Investerum hanterar begäran om radering, se Rutin för hantering av kunders GDPR-begäran.

## 5.5 Konsekvensbedömning (Privacy Impact Assessment)

### 5.5.1 Allmänt om riskanalys och särskild s.k. konsekvensbedömning

Investerum måste alltid göra en inledande riskbedömning innan bolaget påbörjar en behandling av personuppgifter. Denna riskbedömning ska ge svar på hur Investerum bedömer riskerna och, utifrån bedömningen, säkerställer en adekvat skyddsnivå med lämpliga tekniska och organisatoriska åtgärder, allt för att säkerställa, och även kunna visa, att behandlingen utförs enligt dataskyddsregelverket. Utöver kravet på den initiala riskbedömningen krävs i vissa fall att en särskild s.k. konsekvensbedömning genomförs. I den initiala riskbedömningen ska alltid bedömas, och dokumenteras, huruvida risken är sådan att en konsekvensbedömning ska genomföras. Kravet om att utföra konsekvensbedömningar innebär att den personuppgiftsansvarige ska genomföra konsekvensbedömning av sådan behandling av personuppgifter som sannolikt leder till en hög risk för fysiska personers rättigheter och skyldigheter. Bedömningen innebär en kartläggning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

Bolaget har i analysen kommit fram till att man i dagsläget inte behandlar personuppgifter på ett sådant sätt som kräver en konsekvensbedömning enligt Dataskyddsregelverket.

### 5.5.2 När en konsekvensbedömning ska göras

Varje verksamhet bör ha en etablerad process för genomförande av konsekvensbedömningen i syfte att möjliggöra efterlevnad av förordningen. Nedan listas kriterier som ska tas i beaktning om huruvida en konsekvensbedömning ska göras. Om personuppgiftsbehandlingen uppfyller två av dessa kriterier ska en konsekvensbedömning göras:

1) Behandlingen innehåller element av bedömning, profileringar eller värderingar (t.ex. automatiserade kreditbedömningar).

2) Behandlingen syftar till att fatta automatiserade beslut med rättsliga följder eller liknande för den registrerade (t.ex. om behandlingen riskerar att leda till att vissa personer utesluts eller diskrimineras).

3) Behandlingen innefattar systematisk övervakning, vilket anges vara särskilt viktigt eftersom de registrerade ofta inte känner till att vem som samlar in uppgifterna och hur de behandlas.

4) Behandlingen omfattar känsliga personuppgifter (inbegriper även typer av personuppgifter som inte räknas upp i dataskyddsförordningens artikel 9.1 – t.ex. betaluppgifter som kan användas för att begå bedrägerier).

5) Behandlingen innebär att personuppgifter behandlas i stor skala (med beaktande av antalet registrerade som berörs, volymen av uppgifter eller bredden av personuppgiftstyper, behandlingens varaktighet och den geografiska omfattningen av personuppgiftsbehandlingen).

6) Behandlingen innefattar samkörning av uppgifter mellan olika register.

7) Behandlingen omfattar personuppgifter om särskilt utsatta eller skyddsvärda typer av registrerade.

8) Personuppgifterna behandlas på ett innovativt sätt (innefattande behandling med ny teknik) eller för att tillämpa tekniska eller organisatoriska lösningar (t.ex. vid kombinerande av fingeravtryck och ansiktsavläsning för fysisk behörighetskontroll).

9) Personuppgifter ska föras över till ett land utanför EES.

10) Personuppgiftsbehandlingen i sig förhindrar registrerade från att utöva en rättighet eller att använda en tjänst eller ett avtal.

Se Bilaga 5 för närmare vägledning rörande konsekvensbedömning.

### 5.6 Biträden och tredje part

Dataskyddslagstiftningen stadgar att en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning är ett personuppgiftsbiträde.

Med andra ord är den som behandlar personuppgifter för den personuppgiftsansvariges räkning ett personuppgiftsbiträde. Vid anlitande av personuppgiftsbiträden krävs det att ett skriftligt personuppgiftsbiträdesavtal i enlighet med artikel 28 (3) Dataskyddslagstiftningen finns. Det är den personuppgiftsansvarigas skyldighet att enbart anlita personuppgiftsbiträden som uppfyller kraven i Dataskyddsregelverket.

Se Bilaga 6 för avtalspunkter som ska ingå i ett personuppgiftsbiträdesavtal

## 6 Rapportering av personuppgiftsincidenter

### 6.1 Personuppgiftsincidenter

Om en personuppgiftsincident inträffar har Investerum en skyldighet att rapportera incidenten till Integritetsskyddsmyndigheten inom 72 timmar från det att incidenten har skett. I de fall där personuppgiftsincidenten kan anses ha en hög risk för den registrerades fri- och rättigheter har den personuppgiftsansvariga även skyldigheten att informera de berörda registrerade. Se vidare i Bolagets rutinbeskrivning för incidentrapportering.

### 6.2 Rapportering till Integritetsskyddsmyndigheten

Personuppgiftsincidenter som inträffar ska rapporteras till Integritetsskyddsmyndigheten utan onödigt dröjsmål och i den mån det är möjligt inom 72 timmar. Om en anmälan inte kan göras inom 72 timmar ska skälen till att tidsgränsen inte var möjlig att följa anges tillsammans med resterande information i anmälan.

Följande information ska ingå i en anmälan till Integritetsskyddsmyndigheten:

- Personuppgiftsincidentens art och om möjligt antalet registrerade som berörs samt vilken kategori personuppgifterna faller under.
- Kontaktuppgifter till person (VD) där mer information om incidenten kan hämtas lämnas.
- En beskrivning av sannolika konsekvenser till följd av personuppgiftsincidenten.
- Beskriva vilka åtgärder som har/ska tas för att åtgärda personuppgiftsincidenten samt vilka åtgärder som tagits för att minimera de negativa effekterna utav incidenten.

Vidare har Investerum en skyldighet att dokumentera alla personuppgiftsincidenter som sker. I dokumentationen ska omständigheterna kring personuppgiftsincidenten, effekterna av incidenten samt åtgärderna som tagits därefter finnas dokumenterat. Integritetsskyddsmyndigheten har rätt att ta del av dokumentationen. Se vidare i Bolagets rutinbeskrivning för incidentrapportering.

### 6.3 Information till den registrerade

I fall av personuppgiftsincidenter som leder till hög risk för den registrerades fri-och rättigheter måste Bolaget informera den registrerade om personuppgiftsincidenten utan onödigt dröjsmål. Informationen som lämnas måste ge en klar och tydlig bild av personuppgiftsincidentens omfattning och art samt vilka åtgärder Bolaget har eller planerar att ta.

## 7 Fastställande och uppdatering

Dataskyddspolicyn ska minst årligen fastställas av styrelsen även om inga ändringar är påkallade. Beredningsansvarig (IT ansvarig) ansvarar för att policyn minst årligen och löpande vid behov revideras och uppdateras. Vidare är beredningsansvarig ansvarig för att tillse att ägare till styrdokument på lägre nivå får information om förändringar utifrån Dataskyddspolicyn och att förändringar sker.

**Ändringstabell**

| Beslutsform | Rättslig grund | Ändringar i korthet | Antagen | Version |
|---|---|---|---|---|
| Styrelsen | *Dataskyddslagstiftningen* 2018:218, 2018-05-25 | | 2019-12-15 | 1.0 |
| Styrelsen | Dataskyddsregelverket | Ytterligare justering och anpassning till Dataskyddsregelverket. Arbete i verksam-heten kopplad till dataportabilitet fortgår under 2020. | 2019-12-15 | 2.0 |
| Styrelsen | Dataskyddsregelverket | Årlig översyn | 2020-06-17 | 3.0 |
| Styrelsen | Dataskyddsregelverket | Årlig översyn. Ändring av namn på tillsynsmyndighet | 2021-04-20 | 4.0 |

| | | | | |
|---|---|---|---|---|
| | | från Datainspektionen till Integritetsskyddsmyndigheten. | | |
| Styrelsen | Enligt ovan | Årlig översyn | 2022-02-23 | 5.0 |
| Styrelsen | Enligt ovan | Justering av policy i samband med rutinändringar och granskning av funktionen från regelefterlevnad | 2023-04-19 | 6.0 |