RIKTLINJER FÖR

BEHANDLING AV PERSONUPPGIFTER

Fastställd av styrelsen den 10 december 2024

1. Introduktion

Vator Securities AB (”**Vator**” eller ”**Bolaget**”) samlar inom sin verksamhet in och behandlar personuppgifter om exempelvis sina kunder, anställda, konsulter, leverantörer och även också i vissa fall om potentiella kunder och samarbetspartners och omfattas därmed av bestämmelser i Dataskyddsförordningen (Europaparlamentets och rådets förordning (EU) 2016/679, General Data Protection Regulation, även känd som ”GDPR”). Bolagetsmål är att kunder och andra vid all kontakt med Bolaget ska känna sig trygga med hur personuppgifter behandlas. GDPR gäller för *behandling* av *personuppgifter*.

2. Vad är en personuppgift?

En personuppgift är all slags information som kan kopplas till en identifierad eller identifierbar person (en registrerad), såsom namn, personnummer, telefonnummer och adress, men kan även omfatta andra uppgifter som på något sätt går att koppla till en fysisk person, såsom till exempel IP-adress eller registreringsskylt på en privat bil eller en tjänstebil som endast får användas av viss person. Avgörande för om uppgiften anses vara en personuppgift är om uppgiften, enskilt eller i kombination med andra uppgifter, kan knytas till en registrerad.

Exempel på uppgifter som inte anses vara en personuppgift är uppgifter såsom organisationsnummer (med undantag för enskild firma som kan vara personuppgift), allmänna e-postadresser som info@företaget.se, registreringsskylt på en firmabil som kan användas av flera personer etc.

Alla personuppgifter är skyddsvärda men vissa anses mer skyddsvärda än andra. Detta gäller så kallade ”känsliga personuppgifter”. Känsliga personuppgifter är som huvudregel förbjudna att behandla och är uppgifter om

- Etniskt ursprung
- Politiska åsikter
- Religiös eller filosofisk övertygelse
- Medlemskap i fackförening
- Hälsa (uppgifter från t ex tester/undersökningar, sjukdomshistorik, sjukdom, sjukdomsrisk etc)
- Sexualliv eller sexuell läggning
- Genetiska uppgifter (t ex uppgifter från en DNA-analys)
- Biometriska uppgifter vilka används för att entydigt identifiera en person (t ex fingertrycksavläsning, ögonskanning etc)

Utöver känsliga personuppgifter finns ”särskilt skyddsvärda” personuppgifter. Även dessa uppgifter åtnjuter ett mer långtgående skydd än ”vanliga” personuppgifter. Det finns till skillnad från känsliga personuppgifter inget förbud mot behandling dock statueras att en högre säkerhetsnivå kan krävas för att skydda särskilt skyddsvärda personuppgifter. Särskilt skyddsvärda personuppgifter kan vara

- Löneuppgifter
- Uppgifter om lagöverträdelser
- Värderande uppgifter (såsom uppgifter från utvecklingssamtal, resultat från personlighetstester etc)
- Information om persons privata sfär
- Sociala förhållanden

Enligt svensk rätt ges även personnummer och samordningsnummer ett extra skydd. Enligt 3 kap 10 § Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning stipuleras att sådana uppgifter får behandlas utan samtycke endast om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.

3. Vad innebär behandling av personuppgift?

En behandling av en personuppgift är alla typer av åtgärdermed en personuppgift, såsom insamling, registrering, bearbetning, lagring eller radering av personuppgift, oavsett om det sker automatiserat, delvis automatiserat eller manuellt. Om behandlingen sker manuellt (på papper) krävs att uppgifterna ingår eller kommer att ingå i ett manuellt register. För att ett manuellt register ska omfattas av GDPR krävs vidare att informationen är strukturerad så att det enkelt går att hitta information om en enskild person för senare användning.

4. Typ av personuppgifter som Vator Securities samlar in och behandlar

Den typ av personuppgifter som behandlas av Vator Securities består huvudsakligen i kontaktuppgifter till kunder och anställda (den Registrerade) och styrs huvudsakligen av regulatoriska krav som omfattar Vator Securities verksamhet men kan också i vissa fall användas för marknadsföring och information.

Vator Securities är Personuppgiftsansvarig för behandlingen av dessa personuppgifter.

4.1. Kontaktuppgifter

I samband med att en person blir kund hos Vator Securities samlar vi först in personens kontaktuppgifter. Namn, adress, e-postadress, telefonnummer och personnummer, samt en kopia på giltig legitimation.

4.2. Kundprofil

När en person blir kund hos Vator Securities samlas i enlighet med regulatoriska krav viss ytterligare information in, såsom information om kundens ekonomiska situation, kunskap och erfarenhet av investeringstjänster och finansiella instrument, riskaptit, placeringshorisont med mera. För att uppfylla krav på regler för att förhindra penningtvätt och finansiering av terrorism inhämtas också ytterligare uppgifter samt kopia på identitetshandling och görs kontroller mot offentliga register och sanktionslistor med mera.

4.3. Övriga uppgifter som samlas in – ej knutet till kundrelation

Bolaget använder sig av så kallade cookies. Bolaget får därigenom kännedom om vilken sökportal som används mest för att hitta vår webbplats. Vi får också information om man använder sig av dator, surfplatta eller mobil när man söker sig till vår webbplats. Bolaget har en separat cookiepolicy som kan nås via bolagets hemsida.

Personuppgifterna används även för att skicka information som kunden valt att prenumerera på, för att ta emot och registrera anmälningar till våra event, skicka information om erbjudanden och möjlighet att teckna aktier i emissioner.

5. Legal grund för behandling av personuppgifter

5.1 Behandling av personuppgifter ska alltid ske på en laglig grund. Det finns sex legala grunder angivna som kan utgöra grund för tillåten behandling. Följande fyra grunder är relevanta för Vator Securities (övriga har med myndighetsutövning och skydd för registrerad som inte kan lämna samtycke).

Samtycke: Den registrerade har sagt ja till personuppgiftsbehandlingen.

Avtal: Den registrerade har ett avtal eller ska ingå ett avtal med den personuppgiftsansvarige.

Intresseavvägning: Den personuppgiftsansvarige får behandla personuppgifter utan den registrerades samtycke om den personuppgiftsansvariges intressen väger tyngre än den registrerades och om behandlingen är nödvändig för det aktuella ändamålet.

Rättslig förpliktelse: Det finns lagar eller regler som gör att den personuppgiftsansvarige måste behandla vissa personuppgifter i sin verksamhet.

Vilken legal grund som utgör grunden för Bolagets behandling ska dokumenteras i Bolagets register över behandling av personuppgifter.

Om legal grund för en behandling utgörs av en **intresseavvägning** bör VD godkänna den legala grunden innan behandlingen sker.

Om legal grund för en behandling utgörs av **samtycke** krävs att samtycket uppfyller följande krav:

Samtycket ska vara:

a) Tydligt och för ett angivet syfte.
b) Dokumenterat i lämplig form.
c) Lättförståeligt och enkelt att urskilja för den registrerade.
d) Givet genom en aktiv handling. Samtycke i form av underförstått godkännande eller förikryssade rutor är ej giltiga.
e) Jämlikt utifrån maktförhållanden. T ex ska en arbetsgivare inte använda sig av samtycke gentemot en anställd.
f) Möjligt för den registrerade att återkalla när som helst och lika lätt som samtycket är givet. Information om rätten till återkallande ska lämnas till den Registrerade innan samtycke samlas in.
g) Tydligt åtskilt från övriga villkor.
h) Givet av en Registrerad som enligt lag räknas som vuxen. Samtycke kan ej lämnas av minderåriga.

6. Vem har tillgång till personuppgifter?

Anställda på Bolaget har endast tillgång till personuppgifter som är nödvändiga för att fullfölja sitt arbete. Bolaget har flera affärsben vilket gör att personuppgifter ibland finns i flera register. Bolaget har även en del outsourcade funktioner genom konsultavtal, exempelvis IT-tjänster och ekonomi. I dessa funktioner ingår det arbetsmoment där behandling av personuppgifter

förekommer. Alla anställda ingår sekretessavtal och alla konsulter som behandlar personuppgifter på uppdrag av Vator Securities ingår personuppgiftsbiträdesavtal med Bolaget. Sekretessåtaganden i dessa avtal består även om en anställd slutar eller ett konsultuppdrag upphör. Enligt lagen om värdepappersmarknaden är det straffbart att röja personuppgifter till utomstående part.

Insamlade personuppgifter delas också med vissa samarbetsparter, såsom t.ex. emissionsinstitut som biträder med den praktiska hanteringen av nyemissioner.

7. Grundläggande principer för behandling

7.1.1. Vator ansvarar både för att behandling av personuppgifter sker i enlighet med de i GDPR statuerade principerna och för att kunna visa att behandlingen sker enligt förordningen (**ansvarsskyldighet**). Personuppgifter behandlas endast enligt dessa principer:

i) **Laglighet, korrekthet och öppenhet:** Vator Securities ska endast behandla personuppgifter på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade och ska se till att de personuppgifter som behandlas är korrekta och när så krävs uppdaterade (principen om **riktighet**). Det ska vara tydligt för de registrerade att, hur och varför uppgifter behandlas. De registrerade ska vidare få information om sina rättigheter.

ii) **Ändamålsbegränsning:** Vator Securities ska endast behandla personuppgifter för affärsmässiga, uttryckligt angivna, specifika ändamål. Innan insamlande av personuppgifter påbörjas måste Vator Securities avgöra syftet med behandlingen och dokumentera detta i bolagets register över behandling av personuppgifter. Inför ändring av en behandling, exempelvis ett ändrat syfte, måste behandlingen föregås av en ny bedömning innan sådan ändring sker för att säkerställa att den ändrade behandlingen är tillåten enligt gällande lag och denna riktlinje.

iii) **Uppgiftsminimering:** Vator Securities ska endast behandla de personuppgifter som krävs för det aktuella syftet med behandlingen. Personuppgifterna som behandlas ska vara nödvändiga för att uppfylla syftet. Anonymiserade uppgifter ska användas så långt det är möjligt under förutsättning att det inte kräver en orimligt stor insats.

iv) **Lagringsminimering**: Vator Securities ska inte spara personuppgifter längre tid än vad som behövs för att uppfylla det angivna ändamålet eller för att efterleva legala krav. En behandling ska ha en angiven gallringsperiod vilken definierar när personuppgifterna ska raderas eller anonymiseras. Gallringsfrekvens ska finnas angiven i bolagets register över behandling av personuppgifter.

v) **Integritet och konfidentialitet:** Vator Securities ska implementera tekniska och organisatoriska åtgärder för att skydda personuppgifter mot oavsiktlig eller olovlig utplåning, förlust, ändring, spridning eller annan otillåten behandling.

8. Skydd av personuppgifter

8.1. Internt

För de system där personuppgifter registreras krävs det att anställda har en användarprofil. Alla anställda som tar del av Bolagets kunders personuppgifter har egna användare med egenvalda lösenord. Ingen utomstående kan komma åt de personuppgifter som finns i Bolagets register.

8.2. Externt – Personuppgiftsbiträde

För att skydda personuppgifter har Bolaget tecknat tilläggs- eller sidoavtal med respektive personuppgiftsbiträde, som tillgodoser kraven i Dataskyddsförordningen. Dessa avtal innebär exempelvis att personuppgifter inte sprids vidare till tredje part eller att personuppgiftsbiträdet använder sig av personuppgifterna för andra ändamål än vad som framgår av avtalet med personuppgiftsbiträdet.

Vator Securities ska endast anlita ett personuppgiftsbiträde som ger tillräckliga garantier om att personuppgiftsbiträdet genomför lämpliga tekniska och organisatoriska åtgärder för att kunna uppfylla kraven i aktuell lagstiftning samt kunna säkerställa att den registrerades rättigheter skyddas. Ett personuppgiftsbiträde kan exempelvis vara en leverantör av tjänster för outsourcing eller en webbaserad lösning, eller en extern firma som hanterar löneuppgifter på uppdrag av bolaget.

Personuppgiftsbiträdet får endast utföra behandling i enlighet med instruktioner från Vator Securities.

Vator Securities ska endast anlita ett personuppgiftsbiträde för att utföra sådan behandling som bolaget själv har laglig grund att utföra.

Det ska finnas ett skriftligt personuppgiftsbiträdesavtal mellan Vator Securities och varje personuppgiftsbiträde som behandlar personuppgifter på uppdrag av bolaget. Avtalet ska innehålla reglering om att personuppgiftsbiträdet ska skydda personuppgifterna från spridning och att personuppgiftsbiträdet endast ska behandla personuppgifterna i enlighet med Vator Securities instruktioner. Vidare ska avtalet ålägga personuppgiftsbiträdet att implementera lämpliga tekniska och organisatoriska säkerhetsåtgärder för att skydda personuppgifterna samt upprätta rutiner för personuppgiftsincidenter. En mall för personuppgiftsbiträdesavtal bör användas.

Personuppgiftsbiträdet ska omedelbart rapportera personuppgiftsincidenter eller misstanke om sådan incident till Vator Securities.

Personuppgiftsbiträdet ska endast anlita ett underbiträde för behandlingen om personuppgiftsbiträdet erhållit skriftligt godkännande från Vator Securities samt tar ansvar för sådant underbiträdes prestation såsom för sin egen.

9. New Product Approval Process

I samband med processen för godkännande av en ny eller väsentligen förändrad tjänst eller produkt, eller väsentlig utveckling/förändring av Bolagets verksamhet (s.k. NPAP) ska skyddet för personuppgifter beaktas och hanteras

10. Information om personuppgifter

Kunden bestämmer själv över sina personuppgifter och vilka uppgifter som man vill lämna. Samtycke kan återkallas när kunden så önskar.

Observera dock att Vator Securities behöver vissa personuppgifter för att kunna tillhandahålla sina tjänster. Om kund väljer att inte lämna vissa uppgifter eller att återkalla ett lämnat samtycke kan det innebära att Bolaget inte kan tillhandahålla alla sina tjänster eller fullfölja avtal.

Registrerad person har rätt att vända sig till Vator Securities och begära utdrag över vilka egna personuppgifter som Bolaget behandlar samt information om ändamålet med behandlingen och vilka som mottagit personuppgifterna. Om den Registrerade anser att uppgifterna är felaktiga kan denne begära att få sina personuppgifter rättade eller kompletterade. Den Registrerade har även rätt att få sina uppgifter raderade, bl.a. i fall när de inte längre är nödvändiga eller om behandlingen baseras på samtycke och detta har återkallats.

Registrerade personer har även rätt att vända sig direkt till Integritetsskyddsmyndigheten (IMY) om man anser att personuppgifter behandlas i strid med gällande rätt.

Kontaktuppgifter Integritetsskyddsmyndigheten:
Telefonnummer: 08-657 61 00
E-postadress: imy@imy.se

11. Personuppgiftsincident

Med personuppgiftsincident menas en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av personuppgifter. Även ett obehörigt röjande eller obehörig åtkomst till personuppgifter inkluderas i begreppet.

En personuppgiftsincident kan innebära risker för den registrerades fri- och rättigheter & kan få allvarliga konsekvenser, såsom t ex ekonomisk skada, diskriminering, bedrägeri, skadlig ryktesspridning mm. En incident som inte hanteras kan dels leda till att Vators renommé skadas, dels att Integritetsskyddsmyndigheten genom tillsyn utdömer sanktionsavgift.

GDPR kräver att ett företag anmäler vissa typer av personuppgiftsincidenter till IMY. En incident ska anmälas om det inte är osannolikt att incidenten medför risk för fysiska personers fri- och rättigheter. Vator ska alltså vid en eventuell incident göra en bedömning om incidenten ska anmälas till IMY eller inte. Vid bedömningen ska Vator beakta typ av incident, personuppgifternas karaktär och känslighet, hur enkelt det är att identifiera enskilda personer pga incidenten, konsekvensernas svårighetsgrad och vilka samt hur många personer som påverkas. Om Vator efter en sådan bedömning kommer fram till att incidenten ska anmälas måste anmälan lämnas till IMY inom 72 timmar från dess att incidenten upptäcks. Vator ska informera registrerade utan onödigt dröjsmål om bolaget bedömer att incidenten sannolikt leder till en hög risk för den registrerades rättigheter och friheter.

12. Så här behandlas personuppgifter när kundrelation upphör

När kundrelation med Vator Securities upphör tas de personuppgifter som inte kan härledas till något lagkrav på lagring av information bort. Vator Securities informerar även sina samarbetspartners om att uppgifterna ska tas bort och att Bolaget inte längre ska få uppdaterad information om före detta kund.

Kunduppgifter sparas dock minst i 5 år för att Bolaget ska uppfylla vissa lagstadgade krav. Bolaget sparar uppgifterna så länge som det krävs för att Bolaget ska upprätthålla sin tillståndspliktiga verksamhet.

***