| | | | |
|---|---|---|---|
| | Policy för behandling av personuppgifter | | **Rättslig grund**<br>Förordning 2016/679 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).<br>Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning. |
| **Dokumentägare** | **Antagen datum** | **Upprättad av** | **Antagen av** |
| VD | 2018-05-28 | [Legal] | Styrelsen |
| **Dokumenttyp** | **Publiceras** | **Ersätter** | **Version** |
| Policy | Intranätet | | 1.0 |

## 1. Bakgrund

Denna Policy för behandling av personuppgifter (”Policy”) skapar ramverket för instruktioner och rutiner som Pepins Group AB (publ.) (”Pepins” eller ”Bolaget”) har implementerat, eller kommer att implementera, för att säkerställa efterlevnad av för var tid gällande dataskyddslagar.

Denna Policy ska tillämpas på sådan behandling av personuppgifter som helt eller delvis företas på automatisk väg, samt på annan behandling än automatisk av personuppgifter som ingår i eller kommer att ingå i ett register. Policyn omfattar all behandling av personuppgifter som sker med Pepins som personuppgiftsansvarig och som personuppgiftsbiträde.

Denna Policy ersätter i sin helhet Bolagets tidigare interna regler om behandling av personuppgifter.

Vid eventuella motstridigheter mellan Bolagets instruktioner och rutiner, och denna Policy äger vad som anges i detta dokument företräde.

## 2. Gällande regelverk

Europaparlamentets och rådets förordning (EU) 2016/679 av 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 (”GDPR” eller ”dataskyddsförordningen”).

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

## 3. Ansvar

Styrelsen ansvarar för upprättandet av denna Policy. Policyn ska årligen fastställas av Bolagets styrelse även om inga ändringar ska beslutas.

Det åligger VD att tillse att Policyn hålls tillgänglig för samtliga som berörs av den. Ansvaret innebär att tillse att anställda, konsulter, samarbetspartners, ombud och uppdragstagare som berörs av Policyn, känner till och följer innehållet i denna.

Det åligger även VD att fastställa instruktioner som anger hur denna Policy ska genomföras i verksamheten.

Kontroll av efterlevnaden av Policyn ska ske av Bolagets Compliance.

## 4. Definitioner

I denna Policy förekommer ett antal viktiga begrepp, såsom ”registrerade”, ”behandling” och ”personuppgiftsbiträde”. De begrepp som används i Policyn har samma betydelse som i dataskyddsförordningen, om inte något annat uttryckligen framgår.

## 5. Grundläggande principer för behandling

All personuppgiftsbehandling inom Pepins verksamhet ska ske i enlighet med principerna i dataskyddsförordningen och tillämplig svensk lag. Pepins kommer alltid att behandla personuppgifter rättvist och följa de lagar om dataskydd som är tillämpliga på Bolagets verksamhet. Bolaget ska samarbeta vid förfrågningar och utredningar av tillsynsmyndigheten.

Pepins ska behandla personuppgifter på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Det krävs således att laglig grund finns för all behandling av personuppgifter inom Bolaget, samt att den registrerade ska få klar och tydlig information om behandlingen av personuppgifter från Bolaget.

Pepins ska endast samla in personuppgifter för särskilda, uttryckligt angivna och berättigade ändamål. De personuppgifter som samlas in av Bolaget får därefter inte behandlas på ett sätt som är oförenligt med dessa ändamål. Personuppgifter som samlas in av Bolaget ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.

Pepins ska tillse att personuppgifter som behandlas är korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål.

Pepins ska inte förvara personuppgifter 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. Gallring av personuppgifter ska ske när ändamålet med behandlingen är uppfyllt. Vid fastställande av tid för bevarande av personuppgifter måste eventuella lagkrav beaktas.

Pepins ska behandla personuppgifter på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.

Pepins har ett ansvar att påvisa att ovan principer efterföljs. För Bolaget sker detta främst genom denna Policy samt de åtgärder som vidtas utifrån Policyn, såsom upprättande av ett personuppgiftsregister, informationstexter och liknande, men även genom de instruktioner och rutiner som Bolaget har implementerat.

## 6. Personuppgiftsbehandling

Alla personuppgifter är strikt konfidentiella och ska hanteras efter dess känsliga natur. Alla personuppgifter är endast för intern användning, om inte Pepins är tvungna att offentliggöra den i enlighet med en av Bolagets policys, instruktioner och rutiner eller tillämplig lag.

Utgångspunkten i Pepins är att behandling av särskilda kategorier av personuppgifter eller behandling av personuppgifter som rör fällande domar i brottmål samt överträdelser inte ska ske. Behandling av dessa kategorier av personuppgifter får dock ske om det krävs enligt lag eller myndighetsbeslut. Pepins arbete mot penningtvätt och finansiering av terrorism är ett område inom verksamheten som enligt lag kräver att behandling av dessa kategorier av personuppgifter. Vid behandling av särskilda kategorier av personuppgifter eller vid behandling av personuppgifter som rör fällande domar i brottmål samt överträdelser ska lämpliga tekniska och organisatoriska åtgärder vidtas för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken.

Ska behandling av särskilda kategorier av personuppgifter eller vid behandling av personuppgifter som rör fällande domar i brottmål samt överträdelser ske i annat fall krävs att den registrerade uttryckligen lämnat sitt samtycke till behandlingen av personuppgifterna, samt ett godkännande av VD för behandlingen.

Pepins ska endast behandla registrerades personnummer när det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller annat beaktansvärt skäl.

## 7. Behandling av personuppgifter utanför EU/EES

Pepins ska följa de särskilda regler som existerar för överföring av personuppgifter till länder utanför EU och EES. Pepins ska endast överföra personuppgifter som är under behandling eller är avsedda att behandlas efter det att de överförts till ett tredjeland eller en internationell organisation under

förutsättning att; (i) kommissionen har beslutat att tredjelandet, ett territorium eller en eller flera specificerade sektorer i tredjelandet, eller den internationella organisationen i fråga säkerställer en adekvat skyddsnivå, (ii) lämpliga skyddsåtgärder vidtagits, och på villkor att lagstadgade rättigheter för registrerade och effektiva rättsmedel för registrerade finns tillgängliga, eller (iii) något undantag i dataskyddsförordningen är tillämpligt.

Pepins har som utgångspunkt att ingen av verksamhetens behandling av personuppgifter ska ske utanför EU och EES. Undantag för detta måste godkännas av VD.

## 8. Registerförteckning

Pepins ska i enlighet med dataskyddsförordningen föra ett register över Bolagets behandlingar av personuppgifter. Registerförteckningen ska upprättas skriftligen, inbegripet i elektronisk form.

Det är av vikt för Bolagets efterlevnad av dataskyddsförordningen att registerförteckningen är uppdaterad. Uppdatering ska ske vid förändring av en befintlig behandling, och vid upprättandet av nya behandlingar.

På begäran ska Pepins göra registerförteckningen tillgänglig för tillsynsmyndigheten.

## 9. Incidentrapportering

Pepins är skyldiga att till tillsynsmyndigheten, och i vissa fall de registrerade, rapportera säkerhetsincidenter 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 (”personuppgiftsincident”). En personuppgiftsincident ska rapporteras till följd av att denna kan innebära risker för de registrerades integritet.

Vid en personuppgiftsincident ska Pepins utan onödigt dröjsmål och, om så är möjligt, inte senare än 72 timmar efter att ha fått vetskap om den, anmäla personuppgiftsincidenten till tillsynsmyndigheten, såvida det inte är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Om personuppgiftsincidenten sannolikt leder till hög risk för fysiska personers rättigheter och friheter ska Pepins även utan onödigt dröjsmål informera berörda registrerade om personuppgiftsincidenten.

För det fall det inträffar en personuppgiftsincident hos ett av Bolagets personuppgiftsbiträden, måste personuppgiftsbiträdet omedelbart rapportera detta till Pepins.

Pepins ska vidta de åtgärder som krävs för att säkerställa en korrekt hantering av personuppgiftsincidenter.

Dokumentation av inträffade personuppgiftsincidenter ska ske i Bolagets interna incidentregister. För det fall en anmälan av en personuppgiftsincident inte krävs till tillsynsmyndigheten ska dokumentation ändå ske i Bolagets interna incidentregister.

Styrelsen ska av Bolagets Compliance erhålla rapportering om inträffade personuppgiftsincidenter.

## 10. Konsekvensbedömning avseende dataskydd

Pepins är skyldiga att utföra en konsekvensbedömning avseende dataskydd (”DPIA”) 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.

Pepins ska före behandlingen utföra en bedömning av den planerade behandlingens konsekvenser för skyddet av personuppgifter.

Pepins ska vidta de åtgärder som krävs för att säkerställa en korrekt process för utförande av DPIA i enlighet med dataskyddsförordningen i syfte att bedöma risker för Bolagets behandlingar.

Bolagets Compliance ska alltid vara delaktig och rådfrågas i arbetet med DPIA.

## 11. Personuppgiftsbiträden

Om en behandling ska genomföras på Bolagets vägnar ska Pepins endast anlita personuppgiftsbiträden som ger tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen och säkerställer att den registrerades rättigheter skyddas.

För det fall ett personuppgiftsbiträde avser anlita ett annat personuppgiftsbiträde (”underbiträde”) får det inte ske utan ett särskilt eller allmänt skriftligt förhandstillstånd från Pepins. Om ett allmänt tillstånd har använts ska personuppgiftsbiträdet informera Pepins om eventuella planer på att anlita nya underbiträden eller ersätta ett befintligt underbiträde, så att Bolaget har möjlighet att göra invändningar mot sådana förändringar. Underbiträdet ska åläggas samma skyldigheter i fråga om dataskydd som de som fastställs i avtalet med personuppgiftsbiträdet, och framför allt att ge tillräckliga garantier om att genomföra lämpliga tekniska och organisatoriska åtgärder på ett sådant sätt att behandlingen uppfyller kraven i dataskyddsförordningen.

Det ska mellan Pepins och personuppgiftsbiträde upprättas ett skriftligt avtal som avser behandlingen av personuppgifter. Avtalet ska följa de krav som ställs i dataskyddsförordningen, såsom att föremålet för behandlingen, behandlingens varaktighet, art och ändamål, typen av personuppgifter och kategorier av registrerade, samt den personuppgiftsansvariges skyldigheter och rättigheter ska anges. I avtalet ska det även särskilt föreskrivas att personuppgiftsbiträdet;

(i) endast får behandla personuppgifter på dokumenterade instruktioner från Pepins,
(ii) säkerställer att personer med behörighet att behandla personuppgifterna har åtagit sig att iaktta konfidentialitet eller omfattas av en lämplig lagstadgad tystnadsplikt,
(iii) ska vidta alla lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken,
(iv) ska hjälpa Pepins fullgöra sin skyldighet att svara på begäran om utövande av den registrerades rättigheter,
(v) ska bistå Pepins med att se till att skyldigheterna enligt artiklarna 32–36 i dataskyddsförorndingen fullgörs,
(vi) radera eller återlämna alla personuppgifter till Pepins efter det att tillhandahållandet av behandlingstjänster har avslutats,
(vii) ska ge Pepins tillgång till all information som krävs för att visa att personuppgiftsbiträdets skyldigheter har fullgjorts, samt möjliggöra och bidra till granskningar.

I syfte att säkerställa att Bolaget har kontroll över vilka personuppgiftsbiträden som används i verksamheten ska en förteckning över personuppgiftsbiträden finnas.

## 12. Registrerade rättigheter

Till följd av dataskyddsförordningen har registrerade ett antal rättigheter som avser att uppmärksamma och stärka enskilda individers rättigheter i sådana sammanhang i vilka deras

personuppgifter behandlas och registreras. Skydd av varje individs rätt till integritet och rätt att äga sina egna personuppgifter är en grundläggande mänsklig rättighet inom EU. Pepins ska därmed i alla behandling av personuppgifter behandla respektera de registrerade fri- och rättigheter.

Rättigheterna innebär att de registrerade ska få information om när och hur deras personuppgifter behandlas, samt ha kontroll över sina personuppgifter. Registrerade kan således begära att få sina personuppgifter rättade, raderade eller blockerade, men även att få ut eller flytta sina uppgifter.

Pepins ska vidta lämpliga åtgärder för att säkerställa att de registrerades rättigheter kan tillförsäkras. VD ska fastställa en instruktion för hur det i Bolagets verksamhet ska säkerställas att registrerades rättigheter respekteras.

## 13. Inbyggt dataskydd och dataskydd som standard

Pepins ska med beaktande av den senaste utvecklingen, genomförandekostnader och utifrån de integritetsrisker som finns, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder vilka är utformade för ett effektivt genomförande av dataskyddsprinciper och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter skyddas.

Pepins 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.

Pepins ska arbeta på ett strukturerat sätt vid IT-projekt. En riskanalys ska genomföras, och Bolaget ska kartlägga konsekvenserna för integriteten för de personer som registrerats. Kraven på inbyggt dataskydd och dataskydd som standard ska beaktas vid införande av nya IT-system och rutiner, samt även tillämpas på befintliga IT-system och rutiner.

## 14. Utbildning

I syfte att efterleva dataskyddsförordningen och denna Policy ska lämplig utbildning om dataskydd hållas för personal i Pepins som har ständig eller regelbunden tillgång till personuppgifter.

## 15. Andra styrande dokument

Det finns andra styrande dokument inom Bolaget i vilka riktlinjer gällande behandling av personuppgifter utgör en del. För dessa styrande dokument ska vad som stadgas i denna Policy gällande behandlingen av personuppgifter följas.