DATASKYDDSPOLICY

1. Inledning

I samband med sin affärsverksamhet samlar Retta Group Oy och dess dotterbolag (”Retta”) in, använder och lagrar personlig information om sina anställda, kunder, affärspartners och andra fysiska personer. Retta har ett ansvar att säkerställa att bolaget hanterar denna information ansvarsfullt för att skydda individers personuppgifter.

Uppförandekoden är Rettas främsta policy, som samlar alla andra policyer. Olika policyer beskrivs kort i vår uppförandekod och hänvisar till varje specifik policy.

Denna dataskyddspolicy är framtagen för att hjälpa Retta att följa allmänna dataskyddsförordningen (GDPR). Retta ser också till att följa all tillämplig nationell lagstiftning varhelst den är verksam.

Denna policy gäller alla anställda inom Retta-företagsgruppen (”Retta”) och styrelserna för Retta-företagen.

Policyn gäller Rettas alla företag och i alla dess verksamhetsländer. Policyn och tillhörande riktlinjer och arbetspraxis har utformats för att säkerställa att alla anställda är medvetna om och uppfyller sin skyldighet att skydda personers integritet och personliga information samt att säkerställa säkerheten av personuppgifterna.

Retta har även interna anvisningar för sina anställda om dataskydd. I händelse av avvikelser mellan denna policy och andra anvisningar ska denna policy ha företräde.

2. Genomföringen av dataskyddet

Personuppgiftsansvarig	När Retta behandlar personlig information kommer bolaget vanligtvis att göra det på eget initiativ, och avgöra varför och hur den personliga informationen kommer att behandlas, och agera som ”personuppgiftsansvarig”.
Den registrerade	En registrerad är en individ vars personuppgifter behandlas
Gemensamma personuppgiftsansvariga	Ibland kan två eller flera organisationer samarbeta för att bestämma varför och hur personuppgifter behandlas. Detta kallas för ”gemensamma personuppgiftsansvariga” och bör styras av ett gemensamt avtal om personuppgiftsansvariga som bestämmer de personuppgiftsansvarigas respektive ansvar
Personuppgifter	Personuppgifter är upplysningar som avser en identifierad eller identifierbar fysisk person, till exempel namn, personnummer, online-identifikator, lokaliseringsuppgift eller en identifierare såsom deras fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet
Behandling	Behandling är hantering av personlig information, inklusive insamling, användning, bearbetning, överföring, lagring och även radering av personuppgifter.
Personuppgiftsbiträde	Personuppgiftsbiträde betecknar företag som behandlar personuppgifter enbart på uppdrag av och under överinseende av

	ett annat företag. Förhållandena mellan den personuppgiftsansvarige och personuppgiftsbiträdet måste regleras genom personuppgiftsbiträdesavtal (”PUB-avtal”).
Särskilda kategorier av personuppgifter	Vissa kategorier av personuppgifter får i allmänhet inte behandlas, såvida inte särskilda undantag gäller. Dessa kategorier betecknas ibland ”känsliga uppgifter” och inkluderar personuppgifter som avslöjar ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning.

3. Principer för dataskyddet

Vissa principer gäller för varje åtgärd vid databehandling. Retta är skyldig att följa var och en av de principerna som beskrivs nedan.

Korrekthet och laglighet

Retta får endast behandla personuppgifter på vissa specifika rättsliga grunder och måste ta hänsyn till eventuella förhöjda risker för de registrerades integritet.

Uppgiftsminimering och ändamålsbegränsning

Personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål som är förenligt med det ursprungliga skälet för insamlingen av den personliga informationen, och endast i den omfattning som är nödvändig för att uppnå ändamålen. Rettas system och förfaranden bör utformas för att upprätthålla dessa principer.

Riktighet

Retta ska se till att den vidtar aktiva åtgärder för att säkerställa att de personuppgifter som bolaget har registrerat är riktiga och aktuella.

Integritet och konfidentialitet

Retta måste genomföra lämpliga tekniska och organisatoriska åtgärder för att uppnå en säkerhetsnivå som är lämplig för behandlingen av personuppgifter. Retta ska också se till att den upprätthåller integriteten vid behandlingen av personuppgifter och vidtar åtgärder för att förhindra dataförlust genom olyckshändelse. Härvid ska den beakta senaste tillgängliga teknik och kostnaden för genomförandet samt behandlingens art, omfattning, sammanhang och ändamål.

Öppenhet

Bolaget måste se till att det förhåller sig öppet och tillmötesgående till de registrerade om vilken slags personuppgifter bolaget behandlar och hur behandlingen utförs. Öppenhet tillämpas till exempel genom att tillhandahålla information om behandlingsåtgärderna på Rettas webbplats. Alla registrerade personer ska ges information om hurdana personuppgifter som behandlas och på vilket sätt behandlingen utförs. Retta ser till att alla registrerade känner till hur de kan utöva sina rättigheter som registrerade.

Lagringsminimering

Retta måste ha ett systematiskt tillvägagångssätt för att föra register över behandlingen i överensstämmelse med tillämpliga lagar och förordningar, för att skydda sina intressen och för kontinuitet i verksamheten. Personuppgifter får dock inte lagras under onödigt långa perioder om inte ett intresse som hänför sig till den risk detta innebär för personernas integritet väger tyngre.

Ansvarsskyldighet

Principen om ansvarsskyldighet kräver att Retta tar ansvar för och visar efterlevnad vid behandlingen av personuppgifter i enlighet med de principer som beskrivs ovan. Retta ska ha infört lämpliga åtgärder och dokumenterat dessa åtgärder, genom att t.ex. anta och implementera dataskyddspolicyer, upprätthålla dokumentation av behandlingen, genomföra konsekvensbedömningar avseende dataskydd etc.

4. Rättslig grund för behandling av personuppgifter

Retta får endast behandla personuppgifter om den identifierar särskilda rättsliga grunder för behandlingen. Retta bör alltid vara medveten om vilken rättslig grund den förlitar sig på när den behandlar personuppgifter. Mer restriktiva villkor gäller för särskilda kategorier av personuppgifter, såsom förklaras nedan.

Rättslig förpliktelse	Retta får behandla personuppgifter i den omfattning som är nödvändig för att uppfylla en rättslig förpliktelse (t.ex. kundkännedom).
Fullgöra ett avtal	Behandling av personuppgifter är nödvändig för att Retta ska kunna fullgöra sina skyldigheter i ett avtal som den har ingått med den registrerade (t.ex. att behålla bankkontouppgifter för att betala lön enligt ett anställningsavtal), eller för att vidta åtgärder på begäran av den registrerade innan ett avtal ingås.
Bolagets berättigade intresse	Retta får behandla personuppgifter för berättigade ändamål som en del av sin verksamhet (t.ex. att hålla en databas över sina kunder eller affärspartner, eller samla in namn och telefonnummer till nödkontakter för sina anställda). Det berättigade intresset måste dock vara specifikt och motiverat när det vägs upp mot de registrerades grundläggande rättigheter, inklusive deras rätt till privatliv.
Samtycke	Den registrerade ska ha samtyckt till behandlingen. Samtycket ska vara en frivillig, specifik, informerad och otvetydig viljeyttring. De registrerade ska informeras om att de kan återkalla sitt samtycke när som helst.
Övrig	Även om de sällan är tillämpliga, kan det finnas andra grunder för behandling av personuppgifter, nämligen för att skydda intressen som är av grundläggande betydelse för den registrerade eller är av allmänt intresse.

4.1 Rättslig grund för behandling av särskilda kategorier av personuppgifter

Vissa särskilda kategorier av personuppgifter omfattas av extra skydd och får inte behandlas av ett företag utom under specifika omständigheter. Sådana personuppgifter är till exempel upplysningar som avslöjar ras eller etniskt ursprung, politiska åsikter, religiösa eller filosofiska övertygelser, medlemskap i fackförening, eller uppgifter om hälsa, en fysisk persons sexualliv eller sexuella läggning samt vissa former av biometriska uppgifter.

Om särskilda kategorier av personuppgifter behandlas av vilken anledning som helst, ska en högre nivå av dataskydd tillämpas och i vissa fall behövs en konsekvensbedömning avseende dataskyddet.

4.2 Direkt marknadsföring

Vid direkt marknadsföring ska Retta säkerställa att det finns en laglig grund för behandling av personlig information, att registrerade får tillräcklig information om behandlingen och att registrerade kan utöva vissa rättigheter såsom rätten att invända/hoppa av, rätt till tillgång, rätt till rättelse, radering och begränsning.

5. Den registrerades rättigheter och information till de registrerade

Enligt GDPR har de registrerade ett antal rättigheter när det gäller behandlingen av deras personuppgifter. Retta måste beakta dessa rättigheter och se till att ha adekvata rutiner för att tillgodose de registrerades rättigheter.

Förfrågningar från registrerade för att utöva sina rättigheter ska hanteras snabbt, och Retta måste agera på en förfrågan inom en månad efter att den mottogs. I vissa fall kan längre tid vara nödvändig och befogad. Retta är skyldig att vidta alla rimliga åtgärder för att kontrollera den registrerades identitet.

En förfrågan som tas emot av någon anställd på Retta ska alltid omedelbart vidarebefordras till Rettas uppgiftsskyddssamordnare eller lokala uppgiftsskyddssamordnare för vidare åtgärder, enligt Rettas interna instruktioner.

Rätt till information	De registrerade har rätt att få information när personuppgifterna insamlas. Retta har publicerat interna integritetsmeddelanden på företagets intranät, med information om hur det behandlar anställdas personuppgifter. Tredje parter informeras via integritetsmeddelanden som finns på bolagets webbsida.
Rätt till tillträde	Registrerade har rätt att få en bekräftelse på huruvida deras personuppgifter behandlas av Retta eller inte och i så fall få tillgång till sina personuppgifter genom en kopia av de personuppgifter som behandlas (ofta kallad registrerades begäran om tillgång till uppgifter).
Rätt till rättelse, radering ('rätt att bli bortglömd') och begränsning	Den registrerade har rätt att utan onödigt dröjsmål få felaktiga eller ofullständiga personuppgifter som berör hen rättade eller kompletterade. I vissa fall har de registrerade rätt att begära radering av sina personuppgifter (”rätten att bli bortglömd”). Exempel på detta är när samtycke är den rättsliga grunden för behandlingen och den registrerade återkallar sitt samtycke eller om den registrerade visar att uppgifterna inte längre är nödvändiga för de ändamål för vilka de samlades in. Under vissa omständigheter kan registrerade kräva att behandlingen av deras personuppgifter begränsas. Det innebär att Retta endast får lagra personuppgifter och inte behandla dem vidare utan den registrerades samtycke. Rätten till begränsning gäller bland annat när den registrerade anser att uppgifterna är felaktiga och har begärt att de ska rättas. Den registrerade kan då begära att behandlingen av

personuppgifterna begränsas medan deras riktighet kontrolleras. Den registrerade ska informeras när begränsningen upphör.

Rätt att invända — Registrerade har rätt att invända mot Rettas behandling av personuppgifter när behandlingen grundar sig på Rettas legitima intresse. När en registrerad invänder mot behandling av personuppgifter måste Retta upphöra med behandlingen såvida den inte kan visa rättsliga grunder som väger tyngre än den registrerades rättigheter. När personuppgifter behandlas för direkt marknadsföring har de registrerade rätt att när som helst invända mot behandlingen av deras personuppgifter. Om en registrerad motsätter sig behandling av personuppgifter för direkt marknadsföring måste behandlingen för sådana ändamål upphöra.

Rätt till dataportabilitet — Registrerade har rätt att överföra personuppgifter som de har lämnat till Retta till en annan personuppgiftsansvarig (rätten till dataportabilitet) om behandlingen är baserad på avtal eller samtycke, och behandlingen sker automatiserat. Personuppgifterna ska lämnas ut till den registrerade i ett strukturerat, allmänt använt och maskinläsbart format. Om det är tekniskt möjligt kan den registrerade begära att uppgifterna överförs direkt till en annan personuppgiftsansvarig. Rätten gäller endast personuppgifter som den registrerade har lämnat till Retta.

Det finns några undantag där Retta inte är skyldig att tillgodose en begäran som avses ovan, till exempel om en sådan begäran skulle strida mot Rettas rättsliga skyldigheter.

6. Register över behandling

I enlighet med GDPR för Retta ett register över all den behandling av personuppgifter som utförs på Retta. Registret ska innehålla viss information, såsom en beskrivning av kategorierna av personuppgifter och den rättsliga grunden för och ändamålet med behandlingen. Registret ska på begäran lämnas till den behöriga dataskyddsmyndigheten eller andra behöriga dataskyddsmyndigheter.

7. Hantering av personuppgiftsincidenter

Ett personuppgiftsintrång är en säkerhetsincident som resulterar i oavsiktlig eller olaglig förstörelse, förlust, ändring, obehörigt avslöjande av eller tillgång till personlig information som Retta överför, lagrar eller på annat sätt behandlar (t.ex. som ett resultat av dataintrång, ett integritetskänsligt e-postmeddelande till fel mottagare eller ett fel i ett system som gör att data går förlorade). Om det inträffar en personuppgiftsincident som kan medföra en risk för fysiska personers rättigheter och friheter, ska Retta anmäla detta till den behöriga dataskyddsmyndigheten eller den behöriga dataskyddsmyndigheten enligt gällande lagstiftning senast 72 timmar efter intrånget upptäckts, och i vissa fall även informera de registrerade. Ifall personuppgiftsincidenten sannolikt kommer att resultera i en hög risk för fysiska personer, ska Retta även meddela dem om incidenten utan onödigt dröjsmål.

Observera att Retta även kan behöva meddela tredje parter om en incident, såsom försäkringsbolag och behöriga parter i enlighet med avtalsförpliktelser. Retta har interna instruktioner för hantering av dataintrång.

8. Anlita personuppgiftsbiträden och internationella dataöverföringar

Närhelst Retta inleder en relation med en tredje part som innebär utbyte eller överföring av personuppgifter, är Retta skyldig att ingå ett skriftligt avtal med parten. Detta hjälper till att säkerställa att den som behandlar personuppgifter gör det på ett lagligt och ansvarsfullt sätt.

Närhelst Retta utbyter eller överför personuppgifter till en tredje part som personuppgiftsbiträde ska detta ske under ett personuppgiftsbiträdesavtal (PUB-avtal) som ska innehåller vissa villkor. Personuppgiftsbiträde får endast behandla personuppgifter för Rettas räkning enligt anvisningarna i avtalet.

Retta har mallar för PUB-avtal, som anställda på Retta bör använda alltid när det är möjligt.

I tillämpliga fall: Retta ska se till lämpliga skyddsåtgärder vid överföring av personuppgifter utanför EU/EES. Detta kan göras på ett av följande sätt:

Alternativ 1 *Överföring på grundval av ett beslut om adekvat skyddsnivå*	Personuppgifter får överföras utanför EU/EES om kommissionen har beslutat att landet eller organisationen till vilken uppgifterna överförs säkerställer en adekvat skyddsnivå.
Alternativ 2 *Lämpliga skyddsåtgärder*	Om alternativ 1 inte är tillgängligt, bör Retta underteckna ett avtal med den icke-EU/EES-part som använder EU:s standardavtalsklausuler för internationella överföringar (" **SCC** "). Innan Retta ingår i SCC måste Retta granska omständigheterna kring överföringen till en mottagare utanför EU/EES, samt bedöma lämpligheten av personuppgiftsskyddet i mottagarlandet och dokumentera granskningen i en konsekvensbedömning av dataöverföringar ("**TIA**"). Om konsekvensbedömningen påvisar att mottagarlandet utanför EU/EES inte anses säkerställa ett tillräckligt skydd för personuppgifter måste kompletterande åtgärder (juridiska, tekniska eller organisatoriska) vidtas (utöver SCC).
Alternativ 3 *Särskilda undantag*	Om alternativ 1 eller 2 inte används kan personuppgifter överföras utanför EU/EES om ett särskilt rättsligt undantag gäller. Exempel på sådana specifika undantag är: (a) Den registrerade har uttryckligen samtyckt till att uppgifterna får överföras, efter att först ha blivit informerad om de eventuella riskerna med sådana överföringar för den registrerade när det inte föreligger något beslut om adekvat skyddsnivå eller lämpliga skyddsåtgärder, (b) Överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige eller för att genomföra åtgärder som föregår ett sådant avtal på den registrerades begäran, eller (c) Överföringen är nödvändig för att ingå eller fullgöra rättsliga anspråk.

9. Inbyggt dataskydd och dataskydd som standard

Retta måste säkerställa efterlevnad av tillämplig dataskyddslagstiftning (inklusive GDPR) varje gång personuppgifter behandlas. Detta innebär att när IT-system och rutiner utformas måste Retta vidta lämpliga tekniska och organisatoriska åtgärder för att uppfylla kraven i GDPR och skydda den registrerades rättigheter (”integritet enligt avsikt”). Retta måste också se till att personlig information i standardfall inte behandlas i onödan, och inte görs tillgängliga för ett obegränsat antal privatpersoner (integritet som standard).

10. Konsekvensbedömning av dataskydd

Även om det finns en giltig rättslig grund för att behandla personlig information måste Retta först genomföra en dataskyddskonsekvensbedömning (DPIA) om den vill engagera sig i databehandlingsaktiviteter som sannolikt kommer att leda till stora risker för individers frihetsrättigheter (t.ex. installera kameraövervakning i kontorsutrymmen). En konsekvensbedömning av dataskyddet är en process för att identifiera och minimera dataskyddsriskerna som anknyter till behandling. Vänligen kontakta Rettas uppgiftsskyddssamordnare för mer information och/eller instruktioner.

11. Personuppgifter på sociala medier

Närhelst Retta har konton på sociala medieplattformar (t.ex. Facebook, Instagram, Twitter, YouTube, etc.) för kommunikation och marknadsföring, är den personuppgiftsansvarig av behandlingen av personuppgifter på sina egna konton i den omfattning som Retta har kontroll över dessa publikationer och har möjlighet att göra justeringar/radera denna information.

Närhelst Retta använder verktyg som tillhandahålls av en social medieplattform, t.ex. marknadsförings- eller analysverktyg, kan det finnas ett gemensamt ansvar mellan Retta och den sociala medieplattformen.

I den mån Retta är personuppgiftsansvarig ska Retta säkerställa att dess behandling överensstämmer med innehållet i denna anvisning.

12. Användning av kakor på webbplatser och appar

Retta, som webbplats- eller appägare, ansvarar för att ge användarna lämplig information och samla in samtycke innan de använder kakor för att samla in, lagra eller behandla personlig information.

Närhelst Retta använder kakor på sina webbplatser eller appar måste den ha och tillhandahålla en cookiepolicy. Cookiepolicyn ska finnas tillgänglig på webbplatsen eller appen och ska innehålla information till användaren om för vilka ändamål kakor används (t.ex. marknadsföring, statistik eller funktionella kakor), hur informationen som samlas in om användaren behandlas och om informationen är delas med tredje part.

Utöver en cookiepolicy måste webbplatser och appar ha en banner eller popup-formulär som informerar användarna om Rettas cookiepolicy och ber användare att samtycka (eller avvisa) användningen av kakor. Samtycket måste vara specifikt för varje ändamål, och användaren måste samtycka till varje specifik användning.

13. Organisering av dataskyddet

Retta har en dataskyddsorganisation med namngivna ansvariga personer. På koncernnivå leder och ansvarar uppgiftsskyddssamordnaren för Rettas datasekretess. Ett utsett GDPR-kärnteam stöder uppgiftsskyddssamordnaren i sin roll. Uppgiftsskyddssamordnaren har en oberoende position och en rak kommunikationskanal till Rettas styrelse. Lokalt har Retta lokala sekretessteam och en lokal uppgiftsskyddssamordnare i alla länder där Retta är verksamt. Lokala organisationer ansvarar för att bedöma och följa lokala bestämmelser om behandling av personuppgifter. Den lokala uppgiftsskyddssamordnaren rapporterar till uppgiftsskyddssamordnaren och är en del av GDPRs kärnteam. Varje anställd ska känna till denna policy samt relevanta riktlinjer som hör ihop med den.

Alla åtgärder som är i strid med (i) denna policy, (ii) interna riktlinjer eller anvisningar som baseras på policyn eller (iii) dataskyddslagstiftning anses vara dataskyddsöverträdelser. Alla incidenter ska rapporteras på det sätt som beskrivs i avsnitt 15 och undersökas i tillräcklig utsträckning.

14. Engagemang

Varje anställd, chef, och styrelseledamot måste vara införstådd med och följa denna dataskyddspolicy. Cheferna bör se till att deras team är införstådda med och förväntas följa de normer och krav som anges i denna dataskyddspolicy.

Om du har några frågor om innehållet i denna dataskyddspolicy, eller hur den bör påverka ditt vardagliga arbete eller en specifik fråga, vänligen kontakta Rettas uppgiftsskyddssamordnare eller lokala uppgiftsskyddssamordnare.

15. Utbildning

Retta tillhandahåller allmän utbildning till sina styrelseledamöter, ledning och anställda om efterlevnaden av bestämmelserna om dataskydd. Utbildningen upprepas regelbundet.

16. Rapportera misstankar och konsekvenser av överträdelse

Om du blir medveten om eller misstänker ett eventuellt brott mot lag, regel, förordning måste du omedelbart kontakta Rettas chefsjurist.

Om du blir medveten om brott mot denna policy eller någon annan av Rettas policyer, ska du kontakta Rettas Chief Compliance Officer, VD, chef för affärsenheten eller din närmaste chef.

Du kan också rapportera misstankar med Rettas visselblåsartjänst, som finns tillgängligt på Rettas webbplats. Retta tolererar inte några försök att vidta negativa åtgärder mot en anställd som har rapporterat en genuin oro angående misstänkta förseelser. Hämndåtgärder mot en person som rapporterar en oro eller misstanke är ett brott mot uppförandekoden och kommer inte att tolereras.

Retta tolererar inte något olagligt eller oetiskt beteende. Brott mot denna policy kan sannolikt skada Rettas varumärke och rykte. Underlåtenhet att följa denna policy tas på allvar och kan resultera i disciplinära åtgärder som är lämpliga för överträdelsen, inklusive, men inte begränsat till, uppsägning av anställningen.

17. Granskning och uppföljning

Efterlevnaden av denna dataskyddspolicy av alla enheter och anställda inom Retta kommer att övervakas genom interna och externa revisioner och rutinmässiga uppföljningar av alla rapporterade ärenden.

Ikraftträdande datum	Version	Ändra beskrivning
25.5.2018	v1	original
20 december 2023	v2	uppdaterad