DATASKYDDSPOLICY

1. Inledning

I sin affärsverksamhet samlar bolagen i INNA-koncernen in, använder och lagrar personuppgifter om sina medarbetare, kunder, affärspartner och andra personer. INNA har ett ansvar för att hantera denna information på ett ansvarsfullt sätt och skydda enskildas personuppgifter.

Denna dataskyddspolicy syftar till att hjälpa INNA att följa EU:s allmänna dataskyddsförordning (GDPR). INNA säkerställer också att all tillämplig nationell lagstiftning följs i de länder där vi är verksamma.

Denna policy gäller för alla medarbetare i bolagen inom INNA-koncernen (”INNA”) och för styrelserna i INNAs bolag. Policyn gäller för samtliga bolag och verksamhetsländer inom INNA. Denna policy och tillhörande riktlinjer och arbetssätt syftar till att säkerställa att även alla medarbetare känner till och uppfyller sin skyldighet att skydda alla enskildas integritet och säkerheten för deras personuppgifter. INNA har också utfärdat interna anvisningar om dataskydd för sina medarbetare. Vid eventuella motstridigheter mellan denna policy och andra interna anvisningar har denna policy företräde.

I alla dataskyddsfrågor är den primära kontaktpersonen för registrerade den lokalt utsedda roll eller funktion som ansvarar för det löpande dataskydds- och efterlevnadsarbetet.

2. Begrepp inom dataskydd

Personuppgiftsansvarig	Personuppgiftsansvarig är den part som bestämmer ändamålen med och medlen för behandlingen av personuppgifter.
Registrerad	En registrerad är en person vars personuppgifter behandlas.
Gemensamt personuppgiftsansvariga	Ibland kan två eller flera organisationer tillsammans bestämma varför och hur personuppgifter behandlas. Detta kallas gemensamt personuppgiftsansvar och ska regleras i ett avtal om gemensamt personuppgiftsansvar som fastställer parternas respektive ansvar.
Personuppgifter	Med personuppgifter avses varje upplysning som avser en identifierad eller identifierbar fysisk person (”registrerad”). En identifierbar person är en person som direkt eller indirekt kan identifieras, särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift, en online-identifikator eller en eller flera faktorer som är specifika för personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.
Behandling	Med behandling avses hantering av personuppgifter, inklusive insamling, användning, anpassning, överföring, lagring och radering av personuppgifter.
Personuppgiftsbiträde	Ett personuppgiftsbiträde är en organisation som behandlar personuppgifter enbart för en personuppgiftsansvarigs räkning och enligt dennes instruktioner. Förhållandet mellan personuppgiftsansvarig och personuppgiftsbiträde ska regleras i ett personuppgiftsbiträdesavtal.

Särskilda kategorier av personuppgifter	Vissa kategorier av personuppgifter är som huvudregel förbjudna att behandla, om inte särskilda undantag är tillämpliga. Sådana kategorier kallas ibland känsliga personuppgifter och omfattar personuppgifter som avslöjar etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening, samt behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa och uppgifter om en fysisk persons sexualliv eller sexuella läggning.

3. Dataskyddsprinciper

Behandling av personuppgifter måste planeras i förväg. INNAs dataskyddspolicy, riktlinjer och dataskyddslagstiftningen måste följas redan när insamlingen av uppgifter planeras. Den som ansvarar för projektet eller för en förändring av behandlingen ska på ett dokumenterat sätt säkerställa att den registrerades integritet skyddas på lämpligt sätt, med hänsyn till de personuppgifter som ska samlas in och behovet av skydd. INNA måste följa var och en av de principer som beskrivs nedan.

Korrekthet och laglighet

INNA får endast behandla personuppgifter på vissa särskilda rättsliga grunder. Behandlingen måste bygga på lagstiftning, avtal, INNAs berättigade intresse eller någon annan laglig grund för behandling enligt den dataskyddsreglering som nämns i avsnitt 4. Behandlingen ska ta hänsyn till den registrerades berättigade förväntningar och 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 förenliga med det ursprungliga skälet till insamlingen, och endast i den utsträckning som är nödvändig för att uppnå ändamålet. INNAs system och rutiner ska utformas så att dessa principer upprätthålls.

Korrekthet i uppgifterna

INNA måste aktivt säkerställa att de personuppgifter som finns i våra register är korrekta och uppdaterade. Felaktig och inaktuell information ska inte behandlas.

Integritet och konfidentialitet

INNA måste vidta lämpliga tekniska och organisatoriska åtgärder för att uppnå en tillräcklig säkerhetsnivå i sin behandling av personuppgifter. INNA måste också säkerställa integriteten i behandlingen av personuppgifter och vidta åtgärder för att förhindra oavsiktlig förlust av uppgifter. I detta arbete tas hänsyn till relevant modern teknik, kostnaderna för genomförandet samt behandlingens art, omfattning, sammanhang och ändamål.

Öppenhet

INNA måste säkerställa öppenhet gentemot de registrerade om vilka personuppgifter som behandlas, för vilka ändamål, på vilka rättsliga grunder och hur behandlingen sker. Öppenhet uppnås på flera sätt, bland annat genom information om behandlingen på INNAs webbplatser. Alla registrerade ska få information om vilka personuppgifter som behandlas och hur de behandlas. INNA lämnar tydlig och transparent information till registrerade om hur de kan utöva sina rättigheter

Lagringsminimering

INNA måste ha ett systematiskt arbetssätt för att bevara dokumentation i enlighet med tillämpliga lagar och föreskrifter, för att skydda sina intressen och för verksamhetens kontinuitet. Personuppgifter ska dock inte lagras under onödigt lång tid eller utan ett överordnat intresse, med tanke på den risk detta innebär för enskildas integritet.

INNA utvecklar heltäckande rutiner för lagring av personuppgifter utifrån rättsliga krav och särskilt definierade ändamål. Bolaget inför processer för att säkerställa att lagringstiderna följs, vilket innebär att personuppgifter endast får användas så länge det är nödvändigt för ändamålet med behandlingen. När ändamålet upphör förstörs uppgifterna och/eller överförs till arkiv, om inte lagstiftningen ställer särskilda krav på lagring.

INNA åtar sig att införa rutiner för att i rätt tid ta bort uppgifter som har blivit onödiga och inaktuella, och att införa planerade processer för säker förstöring av personuppgifter i enlighet med dataskyddskraven.

Ansvarsskyldighet

Principen om ansvarsskyldighet innebär att INNA ska ta ansvar för och kunna visa att dataskyddsprinciperna ovan följs. Som personuppgiftsansvarig är INNA skyldigt att vidta lämpliga tekniska och organisatoriska åtgärder för att uppfylla kraven på ansvarsskyldighet.

Ansvarsskyldighet kräver lämplig dokumentation. För att uppfylla denna skyldighet måste INNA upprätta och upprätthålla ett internt register över behandling av personuppgifter, hålla externa integritetsmeddelanden uppdaterade, dokumentera personuppgiftsincidenter och genomföra konsekvensbedömningar avseende dataskydd (DPIA) när det krävs. INNA har också åtagit sig att ge sin personal utbildning och anvisningar om dataskydd för att upprätthålla tillräcklig kompetens och, vid behov, kunna visa att sådan utbildning har genomförts.

Datasäkerhet och konfidentialitet

INNA ska vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, med hänsyn till behandlingens art, omfattning, sammanhang och ändamål. Sådana åtgärder kan i förekommande fall omfatta anvisningar och utbildning för personalen, sekretessförbindelser, fysisk säkerhet, behörighetskontroller, säkerhet i informationssystem, loggning och övervakning, kryptering, pseudonymisering eller anonymisering, revisioner och regelbunden granskning av säkerhetsåtgärderna.

Åtkomst till system och databaser som innehåller personuppgifter ska begränsas till behöriga personer som har ett dokumenterat behov av sådan åtkomst i sitt arbete. Behörigheter ska tilldelas, granskas och tas bort i enlighet med tillämpliga rutiner för behörighetshantering.

4. Rättslig grund för behandling av personuppgifter

INNA får endast behandla personuppgifter om det finns en särskild rättslig grund som tillåter behandlingen. Som personuppgiftsansvarig måste INNA alltid känna till vilken rättslig grund som används vid en viss behandling. Personuppgifter får inte behandlas utan en laglig grund. Strängare villkor gäller för särskilda kategorier av personuppgifter, vilket beskrivs nedan.

Rättslig förpliktelse (artikel 6.1 c i GDPR)	INNA får behandla personuppgifter i den utsträckning det är nödvändigt för att uppfylla en rättslig förpliktelse (till exempel skyldigheter om kundkännedom, KYC).
Fullgörande av avtal (artikel 6.1 b i GDPR)	Behandlingen är nödvändig för att INNA ska kunna fullgöra sina skyldigheter enligt ett avtal som ingåtts med den registrerade (till exempel att spara bankkontouppgifter för att betala lön enligt ett

	anställningsavtal), eller för att vidta åtgärder på den registrerades begäran innan ett avtal ingås.
Berättigat intresse (artikel 6.1 f i GDPR)	INNA får behandla personuppgifter när behandlingen är nödvändig för ändamål som rör INNAs eller en tredje parts berättigade intressen, utom när dessa intressen väger lättare än den registrerades intressen eller grundläggande rättigheter och friheter (till exempel att ha en databas med uppgifter om kunder eller affärspartner, eller att samla in medarbetares kontaktuppgifter för nödsituationer). De berättigade intressena måste vara specifika och motiverade vid en avvägning mot de registrerades grundläggande rättigheter, inklusive rätten till integritet. INNA säkerställer denna avvägning genom en intresseavvägning.
Samtycke (artikel 6.1 a i GDPR)	Den registrerade har samtyckt till behandlingen. Samtycket måste vara frivilligt, specifikt, informerat och otvetydigt. Registrerade måste informeras om att de när som helst kan återkalla sitt samtycke.
Övrigt	Även om det sällan är tillämpligt finns det ytterligare grunder för behandling av personuppgifter, nämligen skydd av den registrerades grundläggande intressen och utförande av uppgifter av allmänt intresse.

Rättslig grund för behandling av särskilda kategorier av personuppgifter

INNA behandlar som huvudregel inte särskilda kategorier av personuppgifter, om det inte krävs enligt lag eller är strikt nödvändigt för definierade ändamål. När sådana uppgifter måste behandlas tillämpar INNA förstärkta skyddsåtgärder, inklusive strikta behörighetskontroller, ändamålsbegränsning och säker hantering. Om behandlingen kan innebära en hög risk för enskilda genomförs en konsekvensbedömning avseende dataskydd (DPIA).

Direktmarknadsföring

Vid direktmarknadsföring måste INNA säkerställa att det finns en laglig grund för behandlingen av personuppgifter, att de registrerade får tillräcklig information om behandlingen och att de kan utöva sina rättigheter, inklusive rätten att invända eller avregistrera sig, rätten till tillgång, rätten till rättelse, radering och begränsning. INNA följer lokala regler och marknadspraxis i sin direktmarknadsföring.

5. De registrerades rättigheter och information till registrerade

GDPR ger de registrerade flera rättigheter när det gäller behandlingen av deras personuppgifter. INNA måste iaktta dessa rättigheter och säkerställa att det finns lämpliga rutiner för att tillmötesgå de registrerade.

Förfrågningar från registrerade som vill utöva sina rättigheter måste hanteras skyndsamt, och INNA måste agera på en förfrågan inom en månad från det att den togs emot. I vissa fall kan längre tid vara nödvändig och motiverad. INNA är skyldigt att vidta alla rimliga åtgärder för att kontrollera den registrerades identitet.
En förfrågan som tas emot av någon medarbetare på INNA ska alltid omedelbart vidarebefordras till den lokalt utsedda roll eller funktion som ansvarar för det löpande dataskydds- och efterlevnadsarbetet för vidare åtgärd, i enlighet med INNAs interna anvisningar.

Rätt till information	Registrerade har rätt till information när personuppgifter samlas in. INNAs bolag har publicerat interna integritetsmeddelanden på sina respektive intranät som beskriver hur medarbetares personuppgifter behandlas. Tredje parter informeras genom integritetsmeddelanden som finns på INNAs webbplatser.
Rätt till tillgång	Registrerade har rätt att få bekräftat om deras personuppgifter behandlas av INNA och, om så är fallet, få tillgång till sina personuppgifter genom att få en kopia av de personuppgifter som behandlas (kallas ofta registerutdrag).
Rätt till rättelse, radering (”rätten att bli bortglömd”) och begränsning	Registrerade har rätt att utan onödigt dröjsmål få felaktiga eller ofullständiga personuppgifter om sig själva rättade eller kompletterade. I vissa fall har registrerade rätt att begära att deras personuppgifter raderas (”rätten att bli bortglömd”). Exempel är när samtycke är den rättsliga grunden för behandlingen och den registrerade återkallar sitt samtycke, eller när den registrerade visar att uppgifterna inte längre är nödvändiga för de ändamål som de samlades in för. Under vissa omständigheter kan registrerade begära att behandlingen av deras personuppgifter begränsas. Det innebär att INNA endast får lagra personuppgifterna 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 rättelse. Den registrerade kan då begära att behandlingen av personuppgifterna begränsas medan riktigheten kontrolleras. Den enskilde ska informeras när begränsningen upphör.
Rätt att invända	Registrerade har rätt att invända mot INNAs behandling av personuppgifter när behandlingen grundar sig på INNAs berättigade intressen. När en registrerad invänder måste INNA upphöra med behandlingen, om INNA inte kan visa tvingande berättigade skäl som väger tyngre än den registrerades intressen, rättigheter och friheter. När personuppgifter behandlas för direktmarknadsföring har registrerade en ovillkorlig rätt att när som helst invända mot behandling av sina personuppgifter för sådana ändamål, och INNA måste då upphöra med all behandling för direktmarknadsföring.
Rätt till dataportabilitet	Registrerade har rätt att få ut de personuppgifter som de har lämnat till INNA och att överföra dessa uppgifter till en annan personuppgiftsansvarig (rätten till dataportabilitet), när behandlingen grundar sig på samtycke eller avtal och sker automatiserat. Personuppgifterna måste lämnas i ett strukturerat, allmänt använt och maskinläsbart format. När det är tekniskt möjligt kan den registrerade begära att personuppgifterna överförs direkt till en annan personuppgiftsansvarig. Rätten gäller endast personuppgifter som den registrerade själv aktivt har lämnat till INNA. INNA bedömer varje begäran om dataportabilitet individuellt. Om begäran är uppenbart ogrundad eller orimlig kan INNA vägra att tillmötesgå den eller ta ut en rimlig avgift för att genomföra den. Om INNA avslår en begäran underrättas den registrerade inom en månad från det att begäran togs emot, med angivande av skälen för avslaget och information om möjligheten att lämna in ett klagomål till behörig tillsynsmyndighet.

INNA är inte skyldigt att tillmötesgå registrerades begäranden under vissa omständigheter, bland annat när en begäran skulle strida mot INNAs rättsliga förpliktelser, när begäran är uppenbart ogrundad eller orimlig, eller när tillämplig lag föreskriver särskilda undantag från de registrerades rättigheter.

6. Register över behandling av personuppgifter

I enlighet med GDPR ska INNA föra ett register över all behandling av personuppgifter som utförs inom INNA-koncernen. Registret måste innehålla viss obligatorisk information, bland annat en beskrivning av de kategorier av personuppgifter som behandlas, den rättsliga grunden för behandlingen och ändamålen med behandlingen. Registret ska på begäran göras tillgängligt för berörd dataskyddsmyndighet.

7. Rutin vid personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av, eller obehörigt röjande av eller obehörig åtkomst till, personuppgifter som INNA överför, lagrar eller på annat sätt behandlar (till exempel till följd av dataintrång, ett konfidentiellt e-postmeddelande som skickas till fel mottagare eller ett systemfel som gör att uppgifter går förlorade). Om en personuppgiftsincident inträffar som kan medföra en risk för de registrerades rättigheter och friheter måste INNA anmäla detta till berörd dataskyddsmyndighet enligt tillämplig lagstiftning senast 72 timmar efter att incidenten upptäckts. När en personuppgiftsincident sannolikt leder till en hög risk för en registrerad ska INNA också utan onödigt dröjsmål informera de berörda personerna om incidenten.

Observera att INNA även kan behöva underrätta andra tredje parter om en personuppgiftsincident, till exempel försäkringsbolag och berörda parter enligt avtalsförpliktelser. INNA har fastställt interna anvisningar för hanteringen av personuppgiftsincidenter. Varje medarbetare är skyldig att följa dessa interna anvisningar.

8. Anlitande av personuppgiftsbiträden och internationella överföringar

Ett skriftligt avtal måste ingås mellan personuppgiftsansvarig och personuppgiftsbiträde om behandlingen av personuppgifter. INNA tillhandahåller fastighetsförvaltningstjänster till bostadsbolag och behandlar i samband med detta personuppgifter om boende. Beroende på det enskilda upplägget kan INNA agera antingen som personuppgiftsbiträde för kundbolagets räkning eller som självständigt personuppgiftsansvarig, där kundbolaget är en separat personuppgiftsansvarig.

INNA är personuppgiftsansvarigt när personuppgifter behandlas för INNAs egna affärsändamål, till exempel vid behandling av kontaktuppgifter till företrädare för kundbolag och potentiella kundbolag. Vid utkontraktering av verksamhet anlitar INNA också underleverantörer som kan behandla personuppgifter för INNAs räkning.

Exempel på utkontrakterad behandling av personuppgifter är att köpa databehandlingstjänster (såsom CRM- eller HR-system) från en tjänsteleverantör. När en underleverantör behandlar personuppgifter enligt INNAs instruktioner måste parterna ingå ett skriftligt personuppgiftsbiträdesavtal som anger hur tjänsteleverantören (personuppgiftsbiträdet) behandlar personuppgifter för INNAs räkning och enligt INNAs instruktioner. INNAs ansvar som personuppgiftsansvarig för säkerheten i behandlingen kvarstår även när behandlingen utkontrakteras till en underleverantör. Underleverantören har ingen rätt att behandla uppgifter för egna ändamål och får endast behandla uppgifter inom ramen för uppdraget och i enlighet med INNAs instruktioner.

INNA har tagit fram en standardbilaga om behandling av personuppgifter som vi strävar efter att använda i avtal med underleverantörer. Personuppgiftsbiträdesavtalets innehåll och omfattning beror på

vilken typ av personuppgifter som behandlas, behandlingens omfattning och den riskbedömning som gjorts.

Centrala delar i ett personuppgiftsbiträdesavtal:

• Respektive avtalsparts roll (personuppgiftsansvarig, personuppgiftsbiträde)
• Kategorier av personuppgifter och kategorier av registrerade
• Behandlingen och de specifika uppgifter som personuppgiftsbiträdet ska utföra samt biträdets ansvar
• Uppgifter och ansvar som ligger kvar hos den personuppgiftsansvarige
• Personuppgiftsbiträdets skyldighet att underrätta den personuppgiftsansvarige om planerade förändringar när det gäller underbiträden och att inhämta godkännande för sådana förändringar
• Personuppgiftsbiträdets åtagande att säkerställa att personal som har behörighet att behandla personuppgifter omfattas av sekretessförbindelser
• Nivån på datasäkerheten och tillhörande tekniska och organisatoriska åtgärder samt ansvar
• Radering och/eller återlämnande av personuppgifter när avtalet upphör
• Personuppgiftsbiträdets skyldighet att ge den personuppgiftsansvarige all information som behövs för att visa att skyldigheterna vid behandlingen följs
• Den personuppgiftsansvariges eller dess behöriga företrädares rätt att genomföra dataskyddsrevisioner av personuppgiftsbiträdets verksamhet
• Ett skriftligt avtal måste ingås mellan personuppgiftsansvarig och personuppgiftsbiträde om behandlingen av personuppgifter. Personuppgiftsbiträdet får endast behandla personuppgifter för INNAs räkning i enlighet med personuppgiftsbiträdesavtalet.

När det är tillämpligt måste INNA säkerställa tillräckliga skyddsåtgärder vid överföring av personuppgifter utanför EU/EES. Detta kan göras på något av följande sätt:

Alternativ 1 *Överföring med stöd av ett beslut om adekvat skyddsnivå*	Personuppgifter kan överföras utanför EU/EES om det land eller den enhet som uppgifterna överförs till av EU-kommissionen anses ha en adekvat skyddsnivå.
Alternativ 2 *Lämpliga skyddsåtgärder*	Om alternativ 1 inte är möjligt måste INNA ingå ett avtal med parten utanför EU/EES med hjälp av EU:s standardavtalsklausuler för internationella överföringar (**”SCC”**). Innan SCC ingås måste INNA undersöka omständigheterna kring överföringen till mottagaren utanför EU/EES och bedöma om skyddet för personuppgifter i mottagarlandet är tillräckligt. Denna bedömning måste dokumenteras i en konsekvensbedömning av överföringen **(”TIA”).** Om konsekvensbedömningen visar att mottagarlandet utanför EU/EES inte ger ett tillräckligt skydd för personuppgifter måste kompletterande åtgärder (rättsliga, tekniska eller organisatoriska) vidtas utöver SCC.
Alternativ 3 *Särskilda undantag*	Om alternativ 1 eller 2 inte är möjliga kan personuppgifter överföras utanför EU/EES om ett särskilt rättsligt undantag är tillämpligt. Exempel på sådana särskilda undantag är: (a) uttryckligt samtycke från den registrerade efter att den registrerade har informerats om de möjliga riskerna med en sådan överföring till följd av att det saknas beslut om adekvat skyddsnivå och lämpliga skyddsåtgärder,

(b) överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den personuppgiftsansvarige, eller för att genomföra åtgärder före avtalets ingående på den registrerades begäran,

(c) överföringen är nödvändig för att kunna fastställa, göra gällande eller försvara rättsliga anspråk.

9. Inbyggt dataskydd och dataskydd som standard

INNA tillämpar principerna om inbyggt dataskydd och dataskydd som standard i hela verksamheten. Innan IT-system och rutiner införs måste lämpliga tekniska och organisatoriska åtgärder vidtas för att uppfylla kraven i GDPR och skydda de registrerades rättigheter. Dataskyddskraven identifieras och beaktas i alla processer, tjänster, system och verksamheter och dokumenteras som en del av projektplanen (inbyggt dataskydd). Personuppgifter får inte behandlas i onödan eller i större omfattning än vad som är nödvändigt för det avsedda ändamålet. Denna skyldighet omfattar mängden personuppgifter, lagringstiderna, behandlingens omfattning och uppgifternas tillgänglighet. Uppgifter får inte lämnas ut olagligt eller utan rättslig grund till ett obegränsat antal personer (dataskydd som standard).

10. Konsekvensbedömningar avseende dataskydd

INNA genomför en konsekvensbedömning avseende dataskydd (DPIA) innan behandling inleds som sannolikt leder till en hög risk för enskildas rättigheter och friheter (till exempel installation av kamerabevakning i kontorslokaler). En konsekvensbedömning avseende dataskydd är en process som hjälper till att identifiera och minimera dataskyddsriskerna i en behandling. Kontakta den lokalt utsedda roll eller funktion som ansvarar för det löpande dataskydds- och efterlevnadsarbetet för mer information och/eller anvisningar.

11. Personuppgifter på sociala medier

När INNA har konton på sociala medier (till exempel Facebook, Instagram, Twitter och YouTube) för kommunikation och marknadsföring är INNA personuppgiftsansvarigt för behandlingen av personuppgifter på sina egna konton, i den utsträckning INNA kontrollerar sådana publiceringar och kan ändra eller radera informationen.

När INNA använder verktyg som tillhandahålls av plattformar för sociala medier (till exempel marknadsförings- eller analysverktyg) kan gemensamt personuppgiftsansvar uppstå mellan INNA och plattformsleverantören.
I den utsträckning INNA är personuppgiftsansvarigt måste INNA säkerställa att behandlingen uppfyller kraven i denna policy.

12. Användning av kakor och andra spårningsmetoder på webbplatser och i appar

Som ägare av en webbplats eller app är INNA personuppgiftsansvarigt och ansvarar för att ge användarna lämplig information och inhämta samtycke innan kakor som samlar in, lagrar eller behandlar personuppgifter används.

När INNA använder kakor på sina webbplatser eller i sina appar måste INNA ha och tillhandahålla en kakpolicy. Kakpolicyn måste vara lätt tillgänglig på webbplatsen eller i appen och informera användarna

om för vilka ändamål kakor används (till exempel marknadsförings-, statistik- eller funktionskakor), hur personuppgifter som samlas in om användaren behandlas och om sådan information delas med tredje parter.
Utöver en kakpolicy måste webbplatser och appar visa en banner eller ett popup-formulär som informerar användarna om INNAs kakpolicy och begär användarens samtycke (eller gör det möjligt att avböja) till användningen av kakor. Samtycket måste vara specifikt för varje ändamål, och användarna måste lämna separat samtycke för varje enskild användning av kakor.

13. Roller och ansvar

VD för INNA Group ansvarar för att INNA följer tillämplig lagstiftning i samtliga koncernbolags verksamheter. Detta omfattar efterlevnad av dataskyddslagstiftningen och andra regelverk. VD ansvarar för att dataskyddets styrning och ledning tilldelas inom organisationen.

INNAs ledningsgruppsmedlemmar ansvarar för att dataskyddslagstiftningen följs och integreras i affärsverksamheten, för att dataskyddskraven och de registrerades rättigheter tillgodoses inom deras ansvarsområden och för att tillräckliga resurser avsätts.

Ledningen ansvarar för att medarbetarna får den dataskyddsutbildning som behövs för att kunna utföra sina arbetsuppgifter på ett regelenligt och säkert sätt.
INNAs ledningsgrupp åtar sig också att stödja den lokalt utsedda roll eller funktion som ansvarar för det löpande dataskydds- och efterlevnadsarbetet.

INNA säkerställer att rutiner och policyer för dataskydd upprätthålls och hålls uppdaterade.

Alla medarbetare och chefer ansvarar för att personuppgifter behandlas lagligt. Medarbetare ska löpande få utbildning i dataskydd och vägledning om informationssäkerhet. Varje medarbetare ska följa arbetsgivarens anvisningar vid behandling av personuppgifter och vid genomförandet av dataskyddet. Medarbetare ska identifiera och hantera dataskyddsrisker som rör de egna tjänsterna och uppgifterna och ska följa principerna om inbyggt dataskydd. Varje medarbetare ska rapportera risker eller brister som de upptäcker när det gäller dataskydd eller de registrerades rättigheter till kontaktpersonen för dataskydd eller till sin egen chef.

INNAs intressenter omfattar kunder, samarbetspartner, närstående bolag inom koncernen, leverantörer, underleverantörer och andra relevanta tredje parter. Dataskyddet i leveranskedjan ska regleras genom tillämpliga avtal och dataskyddslagstiftningen.
INNA ska säkerställa att alla parter har tillräcklig information om och förståelse för dataskyddsfrågor. Ledningsgruppen ansvarar för att följa upp efterlevnaden av denna policy. Om du har frågor om innehållet i denna dataskyddspolicy eller om hur den tillämpas, kontakta den lokalt utsedda roll eller funktion som ansvarar för det löpande dataskydds- och efterlevnadsarbetet.

14. Utbildning

INNA erbjuder allmän utbildning för ledning och medarbetare om efterlevnad av dataskyddsreglerna. Utbildning ges löpande. Varje medarbetare ansvarar för att följa INNAs anvisningar om behandling av personuppgifter och för att uppfylla dataskyddskraven.

15. Rapportering av misstankar och konsekvenser av överträdelser

Varje medarbetare är skyldig att rapportera risker eller brister som de upptäcker när det gäller dataskydd eller de registrerades rättigheter till den lokalt utsedda roll eller funktion som ansvarar för det löpande

dataskydds- och efterlevnadsarbetet. Denna rapporteringsskyldighet gäller särskilt personuppgiftsincidenter, som måste rapporteras omedelbart när de upptäcks.

Om du upptäcker en överträdelse av denna policy eller någon av INNAs övriga policyer måste du rapportera det till VD, chefen för affärsenheten eller din chef. Misstankar kan också anmälas via INNAs visselblåsartjänst, som finns på INNAs landsspecifika webbplatser. INNA accepterar inte några försök att vidta negativa åtgärder mot en medarbetare som anmäler en verklig misstanke.
INNA accepterar inte något olagligt eller oetiskt beteende. Överträdelser av denna dataskyddspolicy riskerar att skada INNAs varumärke och anseende. Att inte följa denna dataskyddspolicy ses som allvarligt och kan leda till disciplinära åtgärder som står i proportion till överträdelsen, inklusive men inte begränsat till att anställningen avslutas.

16. Granskning och uppföljning

Att samtliga bolag och medarbetare inom INNA-koncernen följer denna dataskyddspolicy övervakas och granskas löpande, i den omfattning som är lämplig, bland annat genom löpande bedömningar av dataskyddsarbetet. Relevanta frågor som identifieras följs upp internt.

Ikraftträdandedatum	Version	Beskrivning av ändring
25.5.2018	v1	original
20 december 2023	v2	uppdaterad
1 september 2025	v3	uppdaterad
18 juni 2026	v4	uppdaterad