

# Integritetspolicy

## Contents

Syfte .....	2
Definitioner .....	2
Grundläggande principer för Avokis personuppgiftsbehandling .....	3
När behandling av personuppgifter är laglig .....	4
2.1 Allmänt om laglig grund .....	4
2.2 Laglig grund för personuppgiftsbehandling vid rekrytering .....	4
Den registrerades rättigheter .....	5
Lagring och gallring av personuppgifter .....	5
Säkerhet vid behandling av personuppgifter .....	6
5.1 Allmänt .....	6
5.2 Riskanalys .....	6
Överföring av personuppgifter .....	7
6.1 Överföring till personuppgiftsbiträden .....	7
6.2 Överföring till parter med eget personuppgiftsansvar .....	7
6.3 Överföring av personuppgifter till ett tredje land .....	7
6.4 Myndighets begäran om uppgifter .....	7
Rapportering .....	8
Kontaktuppgifter .....	8

## Syfte

Denna integritetspolicy gäller för Avoki HoldCo AB (559039–2311) eller annat bolag som ingår i samma koncern som nu nämnda bolag (hädanefter "Avoki", "vi", "vår", "oss").

Integritetspolicyn har antagits av ledningen och uppdateras vid behov. Policyn utgör allmän information, om hur företaget behandlar interna och externa personuppgifter.

Inom företaget och dess verksamhet hanteras personuppgifter. Uppgifterna behandlas bland annat för att företaget ska kunna fullgöra ingångna avtal med kunder, leverantörer och anställda samt på grund av skyldigheter enligt lag. Som utgångspunkt är Avokis kunder personuppgiftsansvarig för alla behandlingar av personuppgifter som görs under avtal mellan oss och våra kunder. För sådana behandlingar ingår företaget personuppgiftsbiträdesavtal med sina kunder och behandlar uppgifterna under instruktion från och för kundens räkning.

Denna allmänna integritetspolicy ("Integritetspolicyn") gäller när vi behandlar personuppgifter för *egen räkning*, d.v.s. när Avoki är personuppgiftsansvarig. Integritetspolicyn gäller för samtliga anställda och inhyrd personal hos oss inbegripen företagsledning, tjänstemän, anställda och andra personer som agerar för eller på uppdrag av företaget.

Det övergripande syftet med denna integritetspolicy är att fastställa roller och ansvarsområden inom vår organisation, samt att fastställa de normer och principer som ska säkerställa att insamling och behandling av personuppgifter inom företaget sker i enlighet med gällande Dataskyddslagstiftning (enligt definition nedan).

## Definitioner

**Behandling (av personuppgift)** är varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig de sker på automatisk väg eller inte, t.ex. insamling, registrering, organisering, lagring, bearbetning, ändring, begränsning, justering, radering eller förstöring, utlämnande genom översändande, spridning eller annat tillhandahållande av uppgifter, sammanställning eller samkörning.

**Behandlingsregister** avser det register som varje systemägare inom företaget är skyldig att föra över personuppgiftsbehandlingar enligt artikel 30 i GDPR.

**Dataskyddslagstiftning** avser 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 ("GDPR") och varje annan nationell eller europeisk lag, förordning eller direktiv som från tid till annan gäller för företagets behandling av personuppgifter.

**Personuppgifter** är varje upplysning som avser en identifierad eller identifierbar fysisk person som är i livet. Med identifierbar fysisk person menas en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringssuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

**Personuppgiftsansvarig** är den juridiska person som ensam eller tillsammans med andra bestämmer ändamålen med och medlen för behandlingen av personuppgifter.

**Personuppgiftsbiträde** är en juridisk person som behandlar personuppgifter för den personuppgiftsansvariges räkning, t.ex. Avokis leverantörer.

**Integritetsskyddsmyndigheten (IMY)** gör kontroller med anledning av klagomål från enskilda, uppgifter i massmedia eller på eget initiativ. Åtgärder omfattar fältinspektioner och inspektioner genom enkäter eller annan kontroll per e-post, telefon eller brev.

## Grundläggande principer för Avokis personuppgiftsbehandling

Vi ska följa vid var tid gällande Dataskyddslagstiftning vid behandling av personuppgifter.

Vi ska endast behandla personuppgifter på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade och den personuppgiftsansvarige. Detta innebär bl.a. att vår personuppgiftsbehandling ska följa följande grundläggande principer:

- **Dokumenterat personuppgiftsansvar:** För varje behandling av personuppgifter, där vi bestämmer ändamål och medel, ska det finnas ett eller flera bolag inom företaget som har bedömts vara personuppgiftsansvarig. Ansvar för behandlingar där bolag inom företaget är personuppgiftsansvarig ska dokumenteras i Behandlingsregister.
- **Laglig grund:** Varje behandling av personuppgifter ska utföras med stöd av en dokumenterad laglig grund.
- **Ändamålsbegränsning:** Uppgifterna ska samlas in för särskilt, uttryckligen angivna ändamål och får inte senare behandlas på ett oförenligt sätt.
- **Uppgiftsminimering:** Endast personuppgifter som är adekvata, relevanta och inte för omfattande i förhållande till ändamålet ska samlas in.
- **Korrekthet:** Uppgifterna ska vara korrekta och uppdaterade och det ska vara möjligt att spåra ändringar.
- **Lagringsminimering:** Uppgifterna får inte förvaras längre än vad som krävs i förhållande till ändamålet.

- **Konfidentialitet:** Personuppgifter ska skyddas av lämpliga tekniska och organisatoriska säkerhetsåtgärder för att förhindra obehörig eller otillåten behandling och förlust, förstörelse eller förvanskning av uppgifterna.

## När behandling av personuppgifter är laglig

### 2.1 Allmänt om laglig grund

Behandlingen av personuppgifter är endast laglig om minst ett av följande villkor är uppfyllda:

- Den registrerade har **lämnat sitt samtycke** till att dennes personuppgifter behandlas för ett eller flera specifika ändamål.
- Behandlingen är **nödvändig för att fullgöra ett avtal** i vilket den registrerade är part eller för att vidta åtgärder på begäran av den registrerade innan ett sådant avtal ingås.
- Behandlingen är **nödvändig för att fullgöra en rättslig förpliktelse** som åvilar den personuppgiftsansvarige.
- Behandlingen är nödvändig för att **skydda intressen som är av grundläggande betydelse** för den registrerade eller för en annan fysisk person.
- Behandlingen är **nödvändig för att utföra en uppgift av allmänt intresse** eller som ett led i den personuppgiftsansvariges myndighetsutövning.
- Behandlingen är **nödvändig för ändamål som rör den personuppgiftsansvariges eller en tredje parts berättigade intressen**, om inte den registrerades intressen eller grundläggande rättigheter och friheter väger tyngre och kräver skydd av personuppgifter.

Laglig grund för vår behandling av personuppgifter ska avgöras och dokumenteras i den personuppgiftsansvariges Behandlingsregister. Vid osäkerhet ska samråd ske med Avokis General Privacy Manager (GPM).

### 2.2 Laglig grund för personuppgiftsbehandling vid rekrytering

Behandlingen är nödvändig för att kunna hantera ansökan från dig som söker arbete hos oss och baseras på det samtycke som du lämnar i samband med din ansökan. Vi har inget intresse av vetskap av medlemskap i fackförening, trosuppfattning, sexuell läggning, politiska åsikter, eventuella sjukdomar eller andra uppgifter som saknar relevans för rekryteringen, och är därför viktigt att du inte lämnar sådana känsliga personuppgifter i samband med din ansökan eller i en senare kommunikation i rekryteringsprocessen. Personnummer ska inte skickas med, födelsedatum är tillräckligt.

För vissa specifika behandlingar kan du komma att få ytterligare, kompletterande eller avvikande, information om enskild behandling av dina uppgifter.

## Den registrerades rättigheter

En grundläggande aspekt av Dataskyddslagstiftningen är att den innehåller vissa lagreglerade och tvingande rättigheter för de registrerade vars personuppgifter behandlas.

Om en person vill veta vilka uppgifter som finns registrerade om honom eller henne, ska personen inkomma med en skriftlig och egenhändigt undertecknad begäran till Avoki.

Den registrerade har även rätt att återkalla eventuellt lämnade samtycken. Återkallandet av samtycket ska inte påverka lagligheten av behandling som grundar sig på samtycke, innan det återkallas.

Den registrerade har bland annat rätt till:

- Du har **rätt till tillgång** av dina personuppgifter, vilket innebär att du har rätt att få bekräftelse på huruvida personuppgifter som rör dig behandlas och om så är fallet även få tillgång till personuppgifterna och viss ytterligare information om behandlingen.
- Du har **rätt till dataportabilitet**, vilket innebär att du under vissa omständigheter har rätt att få del av sådana personuppgifter om dig som du tillhandahållit till oss, i syfte att du ska kunna överföra personuppgifterna till annan personuppgiftsansvarig.
- Du har **rätt till rättelse, radering eller begränsning** av behandling av dina personuppgifter samt **rätt att invända** mot behandlingen.
- Du har **rätt att klaga** till din nationella dataskyddsmyndighet (i Sverige IMY) om behandling av dina personuppgifter inte uppfyller kraven enligt EU/EES dataskyddslagstiftning.
- Du har **rätt att återkalla ditt samtycke** om och i den mån du lämnat särskilt samtycke till viss behandling.
- Du har **rätt till invändning avseende intresseavvägning** när behandling sker med stöd av så kallad intresseavvägning enligt art. 6.1 f i GDPR.
- Du har **rätt till invändning mot direkt marknadsföring** vid behandling av dina personuppgifter. Då ska personuppgifterna inte längre behandlas för sådana ändamål.

## Lagring och gallring av personuppgifter

Enligt Dataskyddsförordningen får personuppgifter inte lagras längre än vad som är tillåtet enligt lag, eller annars nödvändigt för de ändamål för vilka uppgifterna behandlas. Uppgifter som inte längre får lagras ska permanent raderas och förstöras (gallring). Under särskilda förutsättningar kan gallring genomföras genom att personuppgifterna anonymiseras i stället för att förstöras. Med anonymisering avses att all information som gör det möjligt att spåra uppgifterna till en registrerad, oåterkalleligt raderas.

Om det finns särskilda lagar eller regelverk som kräver lagring av personuppgifter under viss tid, såsom i t.ex. i skatte-, bokförings- eller penningtvättslagstiftningen, gäller sådana bestämmelser före Dataskyddsförordningen. Av bokföringslagen framgår exempelvis att räkenskapsinformation ska sparas i sju år från det år då räkenskapsåret avslutades.

Huvudregeln inom företaget är att personuppgifter som inte omfattas av särskilda lagar eller regelverk (utöver Dataskyddsförordningen) ska gallras när vi inte längre behöver uppgifterna för att uppfylla ändamålet med behandlingen.

## **Säkerhet vid behandling av personuppgifter**

### **5.1 Allmänt**

Avoki ska vidta lämpliga tekniska och organisatoriska åtgärder för att förhindra att personuppgifter förstörs, ändras eller förvanskas. Detta innebär att en säkerhetsbedömning behöver göras från fall till fall och att olika behandlingar/system kräver olika nivå av säkerhetsåtgärder beroende på informationens känslighet, intrångsrisk (och andra risker) samt sårbarhet.

### **5.2 Riskanalys**

Innan vi påbörjar behandling av personuppgifter ska en initial riskanalys genomföras för att ta ställning till:

- Vilka tekniska och organisatoriska säkerhetsåtgärder som är lämpliga för den aktuella behandling, baserat på en bedömning av informationskänslighet, relevanta risker och sårbarhet.
- Om behandlingen är anpassad utifrån och uppfyller vårt krav avseende inbyggt dataskydd (privacy by design) och informationssäkerhet.
- Om behandlingen sannolikt medför en hög risk för de registrerades rättigheter och friheter, t.ex. genom användning av ny teknik eller genom att de registrerade inte kan förväntas känna till att de blir föremål för behandlingen. Om sådan hög risk identifieras ska ansvarig person informeras och avgöra om vidare analys i form av konsekvensbedömning (Data Protection Impact Assessment) är nödvändig.

# Överföring av personuppgifter

## 6.1 Överföring till personuppgiftsbiträden

Avoki kan komma att överföra personuppgifter till extern part, som behandlar personuppgifter för vår räkning och enligt instruktion från oss. Sådan extern part är personuppgiftsbiträde till oss och ska alltid underteckna ett biträdesavtal med Avoki. Avokis General Privacy Manager (GPM) ansvarar för att sådan mall hålls uppdaterad i enlighet med tillämplig Dataskyddslagstiftning från tid till annan.

## 6.2 Överföring till parter med eget personuppgiftsansvar

Avoki kan komma att överföra personuppgifter till annan extern part, som har eget personuppgiftsansvar, under förutsättning att vi har laglig grund för sådan överföring. Sådan laglig grund kan exempelvis vara att överföringen utgör en rättslig skyldighet för oss, eller ett kundavtal som ger oss rätt att överföra uppgifterna.

## 6.3 Överföring av personuppgifter till ett tredje land

Om och i den mån vår personuppgiftsbehandling innebär att personuppgifter överförs till, lagras eller annat sätt behandlas utanför EU/EES-området krävs ytterligare åtgärder för att behandlingen ska vara laglig. Det är tillräckligt att personuppgifterna är nåbara från plats utanför EU/EES, eller att viss infrastruktur eller resurs befinner sig utanför EU/EES, för att ytterligare åtgärder är nödvändiga. Vid överföring av personuppgifter utanför EU/EES-området ska den registrerade informeras om ändamål och omfattning av överföringen.

De åtgärder som vi vidtar för att säkerställa att personuppgiftsbehandling utanför EU/EES är laglig ska alltid dokumenteras och godkännas av Avokis General Privacy Manager (GPM).

## 6.4 Myndighets begäran om uppgifter

Avoki och dess anställda är skyldiga att lämna upplysningar om vår personuppgiftsbehandling och därmed sammanhängande omständigheter om IMY begär det. Även andra myndigheter kan ha rätt att få upplysningar som innehåller personuppgifter från oss, exempelvis Kronofogdemyndigheten, Skatteverket eller Ekobrottsmyndigheten. Det kan också föreligga skyldighet att lämna ut information till polis eller åklagare vid en förundersökning om brott, varvid information endast ska lämnas ut efter skriftlig begäran av förundersökningsledare eller åklagare.

Förutom regelbundna och obligatoriska överföringar av personuppgifter till myndighet som vi har en rättslig skyldighet att rapportera (t.ex. löneuppgifter till Skatteverket och uppgift om



sjukskrivning till Försäkringskassan) ska personuppgifter lämnas ut till myndighet endast efter samråd med Avokis General Privacy Manager (GPM).

Avokis General Privacy Manager (GPM) ansvarar för kontakten med IMY. Alla kontakter med IMY, eller andra myndigheter avseende frågor om personuppgiftsbehandling, för Avokis räkning ska hänvisas till Avokis General Privacy Manager (GPM).

## Rapportering

Avokis General Privacy Manager (GPM) ska årligen eller vid behov rapportera om vår behandling av personuppgifter och därutöver omedelbart rapportera om allvarliga brister, integritetsrisker eller problem uppstår.

Rapporten ska innehålla resultatet av den uppföljning och kontroll av personuppgifter som görs enligt denna Integritetspolicy, inklusive:

- Om behandlingen är anpassad utifrån och uppfyller vårt krav avseende inbyggt dataskydd (privacy by design) och informationssäkerhet.
- Antalet inträffade personuppgiftsincidenter
- Vår efterlevnad av den gällande Dataskyddslagstiftningen och denna Integritetspolicy.
- Eventuella kontakter med Integritetsskyddsmyndigheten; och
- Förändringar av gällande Dataskyddslagstiftning och tillsynspraxis rörande behandling av personuppgifter.

## Kontaktuppgifter

Har du frågor om behandlingen av dina personuppgifter, den här policyn eller om du vill utöva dina rättigheter som har angetts ovan är du välkommen att kontakta oss enligt nedan.

Avoki HoldCo AB (559039–2311)

Attn: DPO

Gustav III: s Boulevard 32, 169 73 Solna

Telefonnummer: 010 – 858 40 00

E-post: [dpo@avoki.se](mailto:dpo@avoki.se)

Detta dokument är godkänt av Avokis ledning.

Detta dokument signeras digitalt.