ARVA

SÄKERHETSÖVERSIKT

Så skyddar Arva dina uppgifter

En översikt över hur vi arbetar med identitet, behörigheter, dokument, artificiell intelligens och skyddet av känsliga uppgifter.

OM DOKUMENTET

Säkerhet börjar med att vara tydlig

Arva hanterar uppgifter om identitet, familj, ekonomi och dödsbon. Det kräver tydliga gränser för vem som får se vad, spårbarhet när något händer och försiktighet när ny teknik används.

Översikten beskriver de skydd som finns i tjänsten i dag. Den är skriven för kunder, anhöriga och samarbetspartners som vill förstå hur uppgifter hanteras utan att läsa teknisk dokumentation.

Dokumentet är ingen certifiering, revisionsrapport eller garanti mot alla risker. Arva är inte ISO 27001-certifierat. När arbetssätt eller teknik förändras uppdaterar vi översikten och versionsnumret.

Våra utgångspunkter

Rätt person	Identitet och behörighet kontrolleras innan känsliga uppgifter lämnas ut.
Minsta åtkomst	Användare och medarbetare ska bara nå den information som behövs för uppgiften.
Kontroll före handling	AI får läsa och strukturera, men viktiga uppgifter ska kunna granskas.
Spårbarhet	Utvalda säkerhets- och ärendehändelser registreras för uppföljning.

INNEHÅLL

Det här går vi igenom

1 Ansvar och grundprinciper 4
2 Identitet och behörighet 5
3 Dokument och personuppgifter 6
4 Tekniskt skydd och spårbarhet 7
5 AI med tydliga gränser 8
6 Leverantörer, rättigheter och kontakt 9

Den aktuella versionen finns alltid på arvaab.se/sakerhet.

1 ANSVAR

Säkerhet är ett löpande ansvar

Säkerhetsarbetet omfattar hur tjänsten byggs, hur behörigheter sätts, hur känsliga uppgifter behandlas och hur avvikelser följs upp. Ansvaret kan inte flyttas till användaren eller till en enskild leverantör.

Principer som styr arbetet

- Dataminimering. Vi samlar inte in mer än vad tjänsten och de rättsliga skyldigheterna kräver.
- Inbyggt dataskydd. Behörighet och avskiljning byggs in i datalagret, inte bara i det som syns på skärmen.
- Flera kontrollager. Identitetskontroll, behörighetsregler, privata filytor och loggning kompletterar varandra.
- Begripliga besked. Säkerhets- och integritetsinformation ska kunna förstås av den som använder tjänsten.
- Försiktighet med juridik. Beräkningar som påverkar bodelning och arv görs med fastställda regler i systemet, inte fritt av en språkmodell.

Avgränsning

Av säkerhetsskäl publicerar vi inte nycklar, interna adresser eller detaljer som kan underlätta angrepp. Sådana uppgifter kan granskas i lämplig form vid en seriös partner- eller säkerhetsprövning.

Vi använder inte formuleringar som antyder en extern certifiering när en sådan inte finns.

2 IDENTITET OCH BEHÖRIGHET

Rätt person ska nå rätt uppgifter

Känsliga familje- och dödsbouppgifter ska inte bli tillgängliga bara för att någon känner till ett namn eller ett ärendenummer. Åtkomst kopplas till en identifierad användare och till rollen i ett visst ärende.

BankID och säker inloggning

Inloggning med BankID sker via en etablerad leverantör för elektronisk identifiering. Flödet skyddas mot att en påbörjad inloggning kapas eller styrs om till en otillåten adress, och signaturen i identitetsintyget kontrolleras innan en session skapas.

Personnummer används där identiteten behöver kopplas till rätt person eller dödsbo. För sökning och matchning används ett kryptografiskt fingeravtryck i stället för personnumret i klartext.

Behörighet per ärende

Åtkomstreglerna finns i databasen och kontrolleras vid varje förfrågan. En användare får bara läsa eller ändra ett dödsbo när en giltig medlems- eller uppdragsrelation finns. Läsbehörighet och redigeringsbehörighet kan skiljas åt.

Administrativa roller hålls i en separat rollstruktur. Kontrollerna sker i databasen och bygger inte på värden som användaren själv kan ändra i webbläsaren.

Delning och återkallelse

När uppgifter delas är åtkomsten knuten till rätt identitet och ett uttryckligt ändamål. Delning kan begränsas och återkallas. Konsumentens arbetsyta hålls åtskild från juristportalens uppdrag och behörigheter.

3 DOKUMENT OCH PERSONUPPGIFTER

Skydd runt varje handling

Ett dödsfallsintyg, testamente, kontoutdrag eller lånebesked kan innehålla uppgifter om flera personer. Uppladdade handlingar behandlas därför som känsligt material genom hela flödet.

Privat lagring	Ärendedokument lagras i privata filytor. Publikt webbmaterial hålls åtskilt från kundhandlingar.
Överföring	Kommunikation mellan webbläsaren, Arva och anslutna tjänster sker över krypterade anslutningar. Hemliga nycklar hanteras i skyddade funktioner.
Inläsning och kontroll	Föreslagna uppgifter jämförs med dokumenttyp och ärendekontext. Viktiga uppgifter visas för kontroll och kan rättas innan de används.
Lagring och radering	Uppgifter sparas så länge de behövs för tjänsten och rättsliga skyldigheter. Konto och dödsbo kan raderas i tjänsten.

Kategorier av uppgifter, rättslig grund och lagringstid beskrivs i Arvas integritetspolicy.

4 TEKNISKT SKYDD

Skyddet ligger i flera lager

Ingen enskild kontroll är tillräcklig. Arva kombinerar identitet, databasregler, privata lagringsytor och skyddade serverfunktioner.

Databasregler	Åtkomst kontrolleras på radnivå så att uppgifter från olika användare, dödsbon och byråer hålls isär.
Serverkontroller	Känsliga operationer kontrollerar session och ärendebehörighet innan uppgifter läses eller ändras.
Begränsade webbanrop	Tillåtna avsändare och returadresser begränsas i relevanta flöden.
Spårbarhet	Utvalda händelser registreras i granskningsloggar. Läsning är begränsad till behöriga roller.
Separata arbetsytor	Konsument, jurist och administration har olika åtkomstvägar och roller.
Kontrollerade ändringar	Förändringar i datamodell och behörighetsregler görs som versionsstyrda ändringar som kan granskas.

Kontrollerna är inget bevis på att risk saknas. Säkerhetsarbete innebär att risker upptäcks, prioriteras och minskas över tid.

5 ARTIFICIELL INTELLIGENS

AI får hjälpa, men inte bestämma

Arva använder AI för att göra stora mängder text och dokument mer begripliga. Tekniken kan läsa, sammanfatta och föreslå uppgifter, men den är inte facit för identitet, juridiska beräkningar eller slutliga handlingar.

Tydliga gränser

- AI ska inte hitta på personnummer, personer eller andra sakuppgifter som saknas i underlaget.
- Beräkningar för bodelning, laglott och efterarv görs av fasta beräkningsregler i systemet.
- Dokumenttyp och källa styr vilka uppgifter som får hämtas. Ett dödsfallsintyg kan vara källa för familjerelationer, en faktura kan det inte.
- Användaren ska kunna se och rätta viktiga uppgifter innan de används i handlingen.
- Planeringsassistenten hålls åtskild från dödsboets uppgifter och ändrar dem inte.

Behandling hos AI-leverantör

När en AI-funktion används skickas det material som behövs för uppgiften till den anslutna tjänsten över en krypterad anslutning. Materialet begränsas till det som uppgiften kräver. Behandlingen beskrivs i integritetspolicyn.

Mänsklig kontroll

AI-genererade svar är vägledning och ersätter inte individuell juridisk rådgivning. Vid komplicerade situationer hänvisar Arva vidare till jurist, och användaren ansvarar för att granska uppgifterna i sin handling.

6 LEVERANTÖRER OCH RÄTTIGHETER

Ansvar följer med uppgifterna

Arva använder specialiserade leverantörer för bland annat drift, elektronisk identifiering, betalning, e-post, signering och AI. Att en leverantör utför en del av tjänsten flyttar inte bort Arvas ansvar att välja lämpliga skydd och beskriva behandlingen.

Leverantörskontroll

Personuppgifter delas bara när det behövs för den aktuella funktionen. Avtal, åtkomst och ändamål begränsar hur uppgifterna får användas. Integritetspolicyn beskriver kategorier av mottagare och skydd vid överföring utanför EU och EES.

Dina möjligheter

Du kan begära tillgång till dina personuppgifter, rättelse, radering, begränsning och i vissa fall dataportabilitet. Du kan även invända mot viss behandling och klaga till Integritetsskyddsmyndigheten.

Kontakt

Säkerhets- och integritetsfrågor besvaras på info@arvaab.se. Skicka inte personnummer eller kontouppgifter i vanlig e-post. Misstänker du obehörig åtkomst, kontakta oss direkt så att vi kan följa upp.

Så skyddar Arva dina uppgifter. Version 1.0, 22 september 2026. Arva AB.