

14. Integritetsskyddspolicy

Hjert-Lungfonden

Beslutad av styrelsen 2025-12-12

Dokumentägare: Generalsekreterare

Dokumentansvarig: Integritetsansvarig

Innehåll

1	Allmänt	2
1.1	Syfte och tillämpningsområde	3
1.2	Integritetsskyddspolicyns giltighetstid.....	3
2	Mål.....	3
3	Roller och ansvar	4
4	Principer för behandling av personuppgifter	5
5	Rättigheter för registrerade	5
6	Personuppgiftsincidenter	6
7	Konsekvensbedömning avseende dataskydd	7
8	Tredjelandsoverföringsbedömning	7
9	Efterlevnad och revidering	7
10	Riktlinjer och arbetsdokument.....	7

1 Allmänt

1.1 Syfte och tillämpningsområde

Syftet med denna policy är att säkerställa att Hjärt-Lungfonden hanterar personuppgifter på ett lagligt, korrekt och transparent sätt i enlighet med GDPR och annan tillämplig dataskyddslagstiftning. Policyn ska skydda individers integritet och säkerställa att deras rättigheter respekteras.

Skydd av personuppgifter är en grundläggande rättighet enligt EU:s stadga om de grundläggande rättigheterna och en viktig del av Hjärt-Lungfondens ansvar gentemot givare, medlemmar, medarbetare och andra intressenter. Hjärt-Lungfonden ska därför behandla personuppgifter ansvarsfullt och i enlighet med gällande lagstiftning och interna styrdokument.

Avgränsning:

- Tekniska och organisatoriska IT-styrningsfrågor regleras i *IT-policyn*.
- Tekniska och organisatoriska åtgärder för informationssäkerhet regleras i *Informationssäkerhetspolicyn*.
- Detaljerade rutiner och operativa processer för dataskydd regleras i *Regelverk för integritetsskydd*, som utgör ett kompletterande styrdokument till denna policy.

1.2 Integritetsskyddspolicyns giltighetstid

Integritetsskyddspolicyn fastställs av styrelsen och gäller från beslutsdagen tills vidare. Policyn revideras minst en gång per år.

2 Mål

Integritetsskyddsarbetet ska:

- skydda individers integritet och personliga rättigheter
- säkerställa att all behandling av personuppgifter har en laglig grund
- säkerställa att personuppgifter samlas in för berättigade syften, att personuppgifterna är relevanta för syftet och att dokumentering av behandlingen sker
- säkerställa att personuppgifter är korrekta, uppdaterade och inte lagras längre än nödvändigt
- säkerställa att personuppgifter skyddas och att personuppgiftsincidenter förebyggs och hanteras
- säkerställa att behandling av personuppgifter kan redovisas öppet och transparent för de registrerade

3 Roller och ansvar

- **Styrelsen** fastställer policyn.
- **Generalsekreteraren** är dokumentägare.
- **Integritetsansvarig** är dokumentansvarig och ansvarar för implementering, uppföljning och bevakning av utvecklingen inom dataskyddsområdet.

- **Integritetsgruppsgruppen** stödjer implementering och uppföljning av dataskyddsfrågor enligt *Regelverk för integritetsskydd* under ledning av Integritetsansvarig.

4 Principer för behandling av personuppgifter

All behandling av personuppgifter ska ske i enlighet med dataskyddslagstiftningens grundläggande principer:

- Laglighet, korrekthet och öppenhet.
- Ändamålsbegränsning - personuppgifter får endast samlas in för särskilda, uttryckligt angivna och berättigade ändamål och får inte behandlas på ett sätt som är oförenligt med dessa ändamål.
- Uppgiftsminimering – endast nödvändiga personuppgifter får behandlas, dvs personuppgifterna ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.
- Riktighet – personuppgifter ska vara riktiga och uppdaterade, felaktiga uppgifter ska rättas eller raderas utan dröjsmål.
- Lagringsbegränsning - uppgifter får inte lagras längre än vad som är nödvändigt för ändamålet för personuppgiftsbehandlingen.
- Integritet och konfidentialitet – personuppgifter ska skyddas mot obehörig eller otillåten behandling, förlust, förstöring eller skada genom tillämpliga tekniska och organisatoriska åtgärder.

Hjärt-Lungfonden tillämpar även principerna:

- Förbud mot hemliga register – register eller uppgifter som medvetet undanhålls från den registrerade. Sådana register får inte inrättas eller användas av Hjärt-Lungfonden.
- Förbud mot otillåten lagring - personuppgifter får inte lagras i format eller på platser där de inte kan uppdateras, versionshanteras, tidsstyras eller omfattas av Hjärt-Lungfondens säkerhets- och åtkomstkontroller. Det är inte tillåtet att skapa eller behålla personuppgifter i egna listor, anteckningar, filer eller utskrifter som ligger utanför dessa verktyg.
- Tillfällig export, pappersanteckningar eller utskrift får endast ske för att utföra ett konkret arbetsmoment och ska därefter förstöras eller lagras digitalt i godkänt system.
- Ändringar, kompletteringar eller radering av personuppgifter ska alltid göras i det ursprungliga systemet.

5 Rättigheter för registrerade

Individ vars personuppgifter behandlas kallas den registrerade och i den egenskapen har individen rättigheterna:

- **Rätt till information** – att bli informerad om hur personuppgifter behandlas.
- **Rätt till tillgång (registerutdrag)** - att få en kopia av sina personuppgifter och information om behandlingen.
- **Rätt till rättelse** - att få felaktiga personuppgifter rättade.
- **Rätt till radering** – att få personuppgifter raderade under vissa förutsättningar.
- **Rätt till begränsning av behandling** – att begära att behandling av personuppgifter begränsas.

- **Rätt till dataportabilitet** – att i vissa fall få ut sina personuppgifter i ett strukturerat allmänt använt och maskininläsbart format och överföra dessa till en annan personuppgiftsansvarig.
- **Rätt att invända mot behandling** – att motsätta sig viss behandling av personuppgifter.

Processer för att hantera dessa rättigheter beskrivs i *Riktlinje för hantering av registrerades rättigheter*.

6 Personuppgiftsincidenter

Alla misstänkta eller konstaterade incidenter som omfattar personuppgifter ska rapporteras omedelbart till integritetsansvarig både via Hjärt-Lungfondens ärendesystem och personligen.

Incidenter innehållande personuppgifter hanteras enligt *Riktlinje för hantering av personuppgiftsincidenter*.

7 Konsekvensbedömning avseende dataskydd

Inför behandling av personuppgifter som medför hög risk för den registrerades rättigheter och friheter ska en konsekvensbedömning (DPIA) genomföras enligt *Riktlinje för konsekvensbedömning av dataskydd*.

8 Tredjelsöverföringsbedömning

Vid behandling av personuppgifter och vid anlitande av personuppgiftsbiträden ska efterlevnad av dataskyddslagstiftning gällande överföring till tredje land säkerställas enligt *Riktlinje för tredjelsöverföringsbedömning (DTIA)*.

9 Efterlevnad och revidering

Policyn följs upp årligen och vid förändringar i lagstiftning.

Avvikelse rapporteras till Generalsekreteraren.

10 Riktlinjer och arbetsdokument

- Regelverk för integritetsskydd
- Riktlinje för hantering av registrerades rättigheter
- Riktlinje för personuppgiftsincidenter
- Riktlinje för personuppgiftsbiträdesavtal
- Riktlinje för konsekvensbedömning avseende dataskydd (DPIA)
- Riktlinje för tredjelsöverföringsbedömning (DTIA)