GDPR-utredning Sveriges Hjärtstartarregister

Sten Bäckström

Version A1

1 juni 2018

Decerno AB
Electrum 234
164 40 Kista
08 630 75 00
info@decerno.se
www.decerno.se
Org. nr: 556498-5025

DECERNO
ADDNODE GROUP

INNEHÅLLSFÖRTECKNING

DECERNO
ADDNODE GROUP

1 SYFTE

Syftet med det här dokumentet är att analysera hur Sveriges hjärtstartarregister (SHR) idag hanterar personuppgifter och vilka åtgärder och ändringar som behöver göras för att uppfylla den nya Dataskyddsförordningen[1]. Syftet är också att utreda vilket ansvar HLR-rådet och Decerno har för detta.

2 BAKGRUND

Denna utredning är baserad på Decernos riktlinjer för anpassning till GDPR.

[1] EU:s Dataskyddsförordning (EU 2016/679), General Data Protection Regulation, GDPR

DECERNO
ADDNODE GROUP

3 SAMMANFATTNING

Här följer en sammanfattning av utredningen:

3.1 Ändamål för insamling av personuppgifter

- SHR samlar in personuppgifter med det särskilda ändamålet att göra hjärtstartare synliga på kartan för att kunna rädda fler liv.
- Ett ytterligare ändamål är att bedriva registerforskning om hjärtstartares placering och användning, baserat på anonymiserad information om hjärtstartare.

3.2 Registrering av användare

- När en användare registrerar sig sparar vi namn, e-post, telefonnummer samt information om huruvida användaren vill ha information via mejl. All denna information behövs för att kunna ge användaren service och kunna upprätthålla kvaliteten i registret, när användaren registrerar hjärtstartare. Användaren ger också sitt uttryckliga, individuella samtycke till att uppgifterna sparas och behandlas. SHR lämnar inte ut användaruppgifter till någon extern part.

3.3 Registrering av hjärtstartare

- När användare registrerar en eller flera hjärtstartare sparar vi en mängd information om hjärtstartaren förutom innehavaren, bland annat position, adress, instruktioner för att hitta den och bilder på var man hittar den, om användaren lägger in sådant. All denna information behövs för att hjärtstartaren ska kunna hittas vid en nödsituation. Informationen kan innehålla personuppgifter om användaren själv skriver in sådan i fritext. Användaren ger inte idag sitt samtycke till att informationen sparas.

3.4 Hur länge sparas informationen?

- Information om användare sparas idag i SHR utan tidsgräns, dvs. även om personen inte har någon aktuell hjärtstartare i systemet så sparas informationen utan tidsgräns.
- Information om en hjärtstartare sparas idag utan tidsgräns, och även om en hjärtstartare tas bort finns den kvar i systemet med status ”Borttagen”

3.5 Vem får del av informationen

- HLR-rådet bedriver registerforskning om hjärtstartares placering och användning, baserat på anonymiserad information om hjärtstartare. HLR-rådet kan också lämna ut anonymiserad information om hjärtstartare till forskningsinstitutioner i syfte att bedriva registerforskning om hjärtstartares placering och användning.
- Generellt utlämnande av information i databasen sker idag på begäran av olika parter. Exempel är datautdrag som beställs av SHR:s support eller av Decerno från olika håll, t.ex. av David Fredman, Sörmlands landsting etc. Decerno har idag inte kontroll över vilka som får begära ut data, utan det sker som beställningar från HLR-rådet.
- Informationen om hjärtstartare i registret delas med tredjepartsutvecklare, t.ex. SMS-livräddarna.
  - En översyn av API:t pågår. Resultaten från den bör inkorporeras i detta dokument innan det slutförs.
  - Vi har fått information om att inga användaruppgifter ska lämnas ut via detta API, enbart information om hjärtstartare.
- Villkoren för API-användare är formulerade så att de inte får spara någon information som de hämtar från oss.

3.6 Samtycke

- Användaren ger idag samtycke till behandling av personuppgifterna vid registrering av användare, men inte vid registrering av hjärtstartare.
- Användaren ges idag ingen samlad information om hur personuppgifterna kommer att behandlas.
- För de uppgifter vi lagrar idag krävs användarens individuella och uttryckliga samtycke under GDPR.

3.7 Otillåten behandling

- Vi utför idag ingen otillåten behandling av uppgifter, dvs. av känsliga personuppgifter.

3.8 Behandlas uppgifterna på ett betryggande sätt?

- Personuppgifterna behandlas idag på ett betryggande sätt.

3.9 De registrerades rättigheter

- Vi kan idag tala om för en användare vilken information som finns lagrad om honom/henne.
- Vi kan idag rätta felaktig information i registret om en användare begär det.
- Vi kan idag radera (glömma) en person ur registret manuellt. Vi har dock inte formulerat en rutin för det.
- Vi avser idag inte att använda personuppgifter för profilering, och HLR-rådet planerar ingen sån behandling för forskning. Om en användare invänder mot automatiserat beslutsfattande och profilering kan vi hävda att sådan inte sker.
- Att flytta personuppgifter till något annat register är inte aktuellt, eftersom det inte finns någonstans att flytta uppgifterna.

3.10 Konsekvensutredning

- Detta dokument är en konsekvensutredning, och visar inte på någon hög risk i samband med lagring och behandling av personuppgifter i SHR. Någon ytterligare konsekevensbedömning behöver inte göras, då vi inte behandlar uppgifter som innebär stor risk för integritetsintrång.

3.11 Miljöer och system

- Personuppgifterna finns i produktionssystemet hos EPM, samt i Decernos testmiljöer. Kraven på dessa miljöer är identiska vad gäller Dataskyddsförordningen.
- Information som kan identifiera en person finns även i systemets loggar.
- Det finns också personuppgifter om användare i HLR-rådets e-postsystem, liksom i Decernos e-postsystem.

DECERNO
ADDNODE GROUP

4 REKOMMENDATIONER

Här följer de rekommendationer som utredningen leder till:

Kommentar [LW1]: Kan vara bra att lägga till någonting om rutin för att rensa/anonymisera loggar?

4.1 Registrering av användare

1. När en användare registreras ska texten ändras till: ”Ja, jag godkänner att ni lagrar och behandlar de uppgifter jag angivit och jag godkänner villkoren.”
2. Ordet «villkoren» ovan ska vara en länk till de villkor som gäller. Se bilaga för utkast till villkor.
3. Villkoren för registrering av **användare** ska formuleras och läggas in på en sida dit länken leder.
4. Villkoren ska innehålla information om hur personuppgifterna används, inklusive att de inte är tillgängliga för samarbetspartners (se bilaga).
5. HLR-rådet kommer inte att använda användarinformation till forskning.
6. HLR-rådet kommer inte att lämna ut information om användare till externa forskare.
7. Det är viktigt att HLR-rådets support slutar lämna ut registerutdrag med användaruppgifter från och med 2018-05-25.
8. Decerno kommer heller inte att lämna ut personuppgifter till andra än HLR-rådet fr.o.m. 2018-05-25.

Kommentar [SB2]: Vi kan inte lämna ut personuppgifter längre p.g.a. GDPR. Viktigt se till att Sandra inte lämnar ut det mer.

4.2 Registrering av hjärtstartare

9. När en hjärtstartare registreras ska en ruta kryssas i med texten: ”Ja, jag godkänner att ni lagrar och behandlar de uppgifter jag angivit och jag godkänner villkoren.”
10. Ordet «villkoren» ovan ska vara en länk till de villkor som gäller. Se bilaga för utkast till villkor. Man ska inte kunna registrera en hjärtstartare utan att rutan kryssas i.
11. Villkoren för registrering av **hjärtstartare** ska formuleras och läggas på en sida dit länken leder (se bilaga).
12. Villkoren ska innehålla information om hur uppgifterna används, inklusive att de är tillgängliga för tredjepartsprodukter (se bilaga).
13. Villkoren ska tydligt deklarera att det förutsätts att inga känsliga personuppgifter finns med i den fria information användaren lägger in, dvs. fritext och bilder (se bilaga).
14. Villkoren ska tydligt påpeka för användaren att om personuppgifter matas in kommer de att vara synliga på kartan, om man inte väljer att göra hjärtstartaren osynlig.
15. I villkoren ska deklareras att anonymiserad information om hjärtstartare kommer att användas till registerforskning om hjärtstartares placering och användning, både av HLR-rådet och externa forskare. Samt att den anonymiserade informationen kommer att kvarstå i registret, men inte vara kopplad till någon person. (Se bilaga.)

4.3 Rutiner för support och förvaltning

16. När HLR-rådets support granskar och kontrollerar registrerade eller ändrade hjärtstartare bör en rutin införas där informationen granskas gällande känslig information samt övriga personuppgifter. I tveksamma fall bör användaren kontaktas och olämpliga personuppgifter tas bort.
17. När HLR-rådets support hjälper en användare att flytta en hjärtstartare från en användare till en annan bör en rutin införas för att i samråd med användaren granska hjärtstartarens information så att inte personuppgifter följer med till den nya användaren. Om det efter ägarbytet finns kvar information som innehåller personuppgifter om den tidigare ägaren ska denna information tas bort.
18. HLR-rådet bör utforma en rutin för att inte spara mejl från användare längre tid än man behöver för att kunna ge service till användare. En riktlinje är att mejl sparas högst ett år.

19. Decerno bör utforma en rutin för att inte spara mejl från användare längre tid än man behöver för att kunna ge service till användare. En riktlinje är att mejl sparas högst ett år.
20. En rutin eller funktion bör inrättas för att ta bort användare ur systemet efter en viss tid om de inte längre har någon aktiv hjärtstartare kopplad till sig. Det bör ske efter maximalt ett år. Detta ska inte gälla administratörer, som ofta inte har någon hjärtstartare registrerad.
21. Om en hjärtstartare är borttagen bör den efter en viss tid anonymiseras, dvs. potentiella personuppgifter tas bort. Innan den tiden har gått kan vi behålla uppgifterna, eftersom vi behöver dem för att kunna aktivera hjärtstartaren igen om användaren så önskar, och därmed ge erforderlig service samt behålla kvaliteten i registret. **Vi behåller följande information**:
    a. Position för ingången
    b. Position för hjärtstartaren
    c. Postnummer
    d. Postort
    e. Anläggningstyp
    f. Våningsplan
    g. Hjärtsäker zon?
    h. Ska hjärtstartaren visas på kartan?
    i. Öppettider

    Vi raderar följande information:

    j. Innehavare/Ansvarig organisation
    k. Namn på hjärtstartaren (valt av användaren, frivilligt)
    l. Gatudress
    m. Instruktioner för att hitta hjärtstartaren (fritext, frivilligt)
    n. Bilder för att hitta hjärtstartaren (användarens egna bilder, frivilligt)
    o. Vilken person (användare i systemet) hjärtstartaren är kopplad till
22. En rutin eller funktion för att glömma en användare ska införas. Alla personuppgifter i systemet ska tas bort eller anonymiseras. Det innefattar både den information användaren matat in samt information i loggar.
    a. Decerno upprättar en manuell rutin, vilket kräver lite mer tid varje gång, eftersom vi inte förväntar oss många fall
    b. Det är möjligt att i framtiden utveckla en automatisk funktion för att glömma en användare, vilket tar lite längre tid att utveckla, men gör att HLR-rådet själva kan glömma en användare med en knapptryckning, eller att användaren själv kan göra det i gränssnittet.
23. Vi bör formulera en enkel sammanställning över exakt vilka personuppgifter vi lagrar om en användare, så att vi lätt kan meddela det vid förfrågningar.
24. Personuppgiftsbiträdesavtal ska tecknas av HLR-rådet med Decerno.
25. HLR-rådet ska teckna personuppgiftsbiträdesavtal med EPM.
26. En rutin för personuppgiftsincidenter ska upprättas. Det kan vara en enkel instruktion.

Kommentar [LW3]: Om man är admin har man generellt ingen aktiv hjärtstartare (men det är kanske endast ett undantagsfall som inte behöver tas upp här)?

Kommentar [SB4]: Detta är en av få utestående punkter: Ska position betraktas som personuppgift?

DECERNO
ADDNODE GROUP

5 LAGLIG BEHANDLING AV PERSONUPPGIFTER

Här börjar en mer detaljerad genomgång, vilken är underarbetet till ovanstående sammanfattning och rekommendationer.

Detta avsnitt täcker riktlinjerna för laglig behandling av personuppgifter, samt ger en analys av hur SHR lever upp till riktlinjerna.

5.1 Ändamål för insamling av personuppgifter

Personuppgifter får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Följande är HLR-rådets särskilda ändamål och berättigande:

SHR samlar in personuppgifter med det särskilda ändamålet att göra hjärtstartare synliga på kartan för att kunna rädda fler liv.

5.2 Grundläggande principer

Grundläggande principer inom integritetsskydd är att man måste ha ett behov av den information man samlar in. Mer specifikt gäller att:

27. Inte samla in mer information än vad som behövs
28. Inte ha kvar informationen längre än nödvändigt
29. Inte använda uppgifter till något annat än vad som var syftet när de samlades in
30. Har den registrerade lämnat sitt samtycke till behandling av personuppgifterna är behandling i regel tillåten. Ett samtycke ska vara individuellt, frivilligt och tydligt
31. Den registrerade ska innan samtycket ha informerats om tilltänkt behandling av lämnade personuppgifter
32. Den registrerade kan när som helst återkalla sitt samtycke varefter behandling inte längre får ske
33. I några fall krävs inte samtycke enligt artikel 6 i dataskyddsförordningen. Detta gäller för nödvändig behandling, t.ex. för att fullgöra lagliga åtaganden.

Nedan går vi igenom dessa principer och analyserar hur SHR lever upp till dem idag.

5.3 Behov av personuppgifter

Man inte får samla in mer information än vad som behövs.

SHR samlar idag in följande information:

5.3.1 Insamlade personuppgifter

- Förnamn
- Efternamn
- E-post
- Telefonnummer
- Extra telefonnummer
- Information om att användaren vill ta emot nyheter via mejl

Av dessa uppgifter är alla obligatoriska utom «Extra telefonnummer».

Alla dessa uppgifter har SHR behov av för att kunna identifiera användaren, nå användaren när det behövs för validering av hjärtstartaren, och för att kunna ge nödvändig service till kunden. Vår support behöver ofta nå kunden via olika kanaler för att kunna ge den service som krävs. Informationen behövs, kort sagt, för att

kunna hålla ett kvalitetssäkert register över Sveriges hjärtstartare. Ett kvalitetssäkert register har vi när vi vet att hjärtstartaren finns där den finns, och att vi kan kontrollerar det genom en kontaktperson.

5.3.2 Insamlade uppgifter om hjärtstartare

SHR samlar också in en mängd uppgifter om varje hjärtstartare. Här går vi igenom den informationen. Syftet är att identifiera om det finns personuppgifter bland dessa.

SHR samlar in följande information om varje hjärtstartare:

- Innehavare/Ansvarig organization
- Namn på hjärtstartaren (valt av användaren, frivilligt)
- Position för ingången
- Position för hjärtstartaren
- Adress
- Postnummer
- Postort
- Anläggingstyp (begränsat urval ur lista)
- Våningsplan
- Är hjärtstartaren del av en hjärtsäker zon? (frivilligt)
- Instruktioner för att hitta hjärtstartaren (fritext, frivilligt)
- Bilder för att hitta hjärtstartaren (användarens egna bilder, frivilligt)
- Ska hjärtstartaren visas på kartan?
- Öppettider
- Vilken person (användare i systemet) hjärtstartaren är kopplad till

5.3.2.1 Behov av uppgifter om hjärtstartare

Här följer en genomgång och analys av all information ovan som vi sparar om en hjärtstartare. För varje typ av information anges behovet, samt vilken typ av personuppgifter som kan ingå.

Innehavare/Ansvarig organization. Denna information beskriver vilken organisation eller person som äger hjärtstartaren.

- Behov: Att kunna ge service och ha ett kvalitetssäkert register.
- Här kan personlig information finnas, beroende på vad användaren skriver. Om detta är ett företagsnamn är det kanske inte personuppgifter. Men det kan t.ex. vara ett personnamn, eller ett namn på ett enmans- eller fåmansföretag. Då är det möjligt att identifiera en person och det är därmed en personuppgift.

Namn på hjärtstartaren (valt av användaren, frivilligt). Denna information ges som service till användaren för att en användare med flera hjärtstartare lätt ska kunna skilja dem åt.

- Behov: Denna information är frivillig och ges som en service till användaren. Den behövs för att användaren ska kunna hålla reda på sina hjärtstartare i registret.
- Här kan personlig information finnas, beroende på vad användaren skriver i fritext. Det är ju t.ex. möjligt att användaren skriver in ett personnamn här.

Position för ingången

- Behov: Den som ska använda hjärtstartaren, t.ex. SOS Alarm, ska kunna hitta till ingången. Denna information används inte idag, men den kommer att bli viktig i framtiden.

- Detta kan vara en personuppgift i kombination med annan information, t.ex. namn, telefonnummer etc. Enbart positionen bedömer vi dock inte är en personuppgift. En geografisk punkt i sig är ingen personuppgift.

Position för hjärtstartaren

- Behov: Den som ska använda hjärtstartaren, t.ex. SOS Alarm, ska kunna hitta till hjärtstartaren.
- Detta kan vara en personuppgift i kombination med annan information, t.ex. namn, telefonnummer etc. Enbart positionen bedömer vi dock inte är en personuppgift. En geografisk punkt i sig är ingen personuppgift.

Adress

Postnummer

Postort

- Behov: Adress, postnummer och postort behövs för att kunna ange var hjärtstartaren finns för den som ska hitta den.
- Adress är en personuppgift om man med den kan identifiera en person. Det kan vara en personuppgift om adress, postnummer och ort ingår. Enbart postnummer och postort är ingen personuppgift.

Anläggingstyp (begränsat urval ur lista)

- Behov: För att kunna ha tillförligtlig statistik kring var hjärtstartare finns.
- Detta är inte någon personuppgift.

Våningsplan

- Behov: Den som ska använda hjärtstartaren, t.ex. SOS Alarm, ska kunna hitta till hjärtstartaren.
- Detta är inte någon personuppgift.

Är hjärtstartaren del av en hjärtsäker zon?

- Behov: Visa på kartan att hjärtstartaren ingår i en hjärtsäker zon. Det är användaren som själv, frivilligt markerar detta, och det är i användarens eget intresse att visa att man tillhör en hjärtsäker zon.
- Detta är inte någon personuppgift.

Instruktioner för att hitta hjärtstartaren (fritext, frivilligt)

- Behov: Den som ska använda hjärtstartaren, t.ex. SOS Alarm, ska kunna hitta till hjärtstartaren.
- I det här fältet är det inte tänkt att det ska finnas några personuppgifter, men det kan ändå hända att användaren själv väljer att skriva in information som innehåller personuppgifter, t.ex. personnamn, telefonnummer eller liknande.

Bilder för att hitta hjärtstartaren (användarens egna bilder, frivilligt)

- Behov: Den som ska använda hjärtstartaren, t.ex. SOS Alarm, ska kunna hitta till hjärtstartaren.
- Bilder ska normalt inte innehålla någon personinformation, men det kan vara fallet att användaren lägger in en bild med en person på, alternativt en plats eller ett hus som är tydligt identifierbart, och därmed kan identifiera en person.

Ska hjärtstartaren visas på kartan?

- Behov: Att försäkra oss om att den användare som inte vill att hjärtstartaren ska visas på kartan kan få sin önskan tillgodosedd. Detta är i användarens intresse.
- Detta är inte en personuppgift.

Öppettider

- Behov: Den som ska använda hjärtstartaren, t.ex. SOS Alarm, ska veta när hjärtstartaren är tillgänglig
- Detta är inte en personuppgift.

Vilken användare hjärtstartaren är kopplad till

- Behov: Vi behöver en kontaktperson för att kunna hålla ett kvalitetssäkert register (se sektion **Fel! Hittar inte referenskälla.**).
- Denna koppling är en personuppgift, men dessa personuppgifter behandlas under **Fel! Hittar inte referenskälla.**.

5.3.3 Testversion

Decerno har en testversion av SHR som innehåller en kopia på delar av produktionsdatabasen. Denna testversion innehåller samma typ av information som produktionssystemet. Testversionen hanteras av Decernos utvecklare parallellt med produktionssystemet. Det finns ingen skillnad i datasäkerhet mellan produktionssversion och testversion. De behöver behandlas på samma sätt vad gäller Dataskyddsförordningen.

5.3.4 Övrig insamlad information

Följande information finns också i SHR:

- Systemets loggar
  - Behov: Vi behöver information i loggar för att kunna underhålla systemet.
  - Loggar innehåller personuppgifter.

5.3.4.1 Information extern för systemet

Följande information samlas av HLR-rådet eller Decerno, men är inte en del av SHR:

- Mejl som skickas av användare till rådets medlemmar, framför allt mejl till info@hjartstartarregistret.se
- Mejl som skickas vidare av HLR-rådets personal till Decerno eller andra, där användares personuppgifter finns med. Det är främst uppgifter som finns i registrets databas, men kan även vara vilken information som helst som användaren skrivit i sina mejl till supporten, och som sen vidarebefordras till Decerno eller annan part.

5.4 Hur länge sparas uppgifterna

Inte ha kvar information längre än nödvändigt

Följande gäller för hur länge systemet sparar ovanstående uppgifter:

5.4.1.1 Personuppgifter

Personuppgifter om användare sparas idag utan tidsgräns. Administratör kan ta bort en användare.

5.4.1.2 Uppgifter om hjärtstartare

Information om hjärtstartare sparas idag utan tidsgräns. När en hjärtstartare tas bort markeras den som borttagen, men sparas fortfarande. Administratör kan inte ta bort hjärtstartaren ur databasen.

5.5 Hur används personuppgifterna?

Inte använda uppgifter till något annat än vad som var syftet när de samlades in.

Sveriges Hjärtstartarregister använder inte informationen för något annat ändamål än för det den samlades in. Syftet med insamlingen av uppgifter är:

Att göra hjärtstartare synliga på kartan för att kunna rädda fler liv.

Att i syfte att rädda fler liv kunna hålla ett kvalitetssäkrat register

Att för att kunna hålla ett kvalitetssäkrat register ha möjlighet att kontakta innehavare av hjärtstartare.

Att i syfte att kunna ge service till användare av registret kunna kontakta användare

Att bedriva registerforskning om hjärtstartares placering och användning baserad på anonymiserad information om hjärtstartare.

5.6 Samtycke

Har den registrerade lämnat sitt samtycke till behandling av personuppgifterna är behandling i regel tillåten. Ett samtycke ska vara individuellt, frivilligt och tydligt.

När en ny användare skapas i systemet godkänner användaren att uppgifterna sparas och behandlas genom att kryssa i rutan med texten:

«Ja, jag godkänner att ni lagrar och använder de uppgifter jag angivit»

Vi har alltså användarens samtycke. Samtycket är individuellt, frivilligt och tydligt.

För att vara extra tydlig är det lämpligt att byta ut ordet «använder» mot «behandlar», som är den formella termen.

Obs! Vid registrering av en hjärtstartare ger användaren inget samtycke, trots att det kan lagras personliga uppgifter. Det finns också en risk att användaren matar in oönskad information. Användaren borde godkänna villkoren även vid registrering av hjärtstartare.

5.7 Information till den registrerade

Den registrerade ska innan samtycket ha informerats om tilltänkt behandling av lämnade personuppgifter.

När användaren godkänner lagring och behandling av sina uppgifter – både för person och hjärtstartare – bör användaren få läsa ett avtal om hur uppgifterna behandlas. Detta sker inte idag.

Här är det viktigt att det även ingår information om att tredjepartssystem, som SMS-livräddarna ingår i beskrivningen.

Information om forskning på uppgifterna ska också tillhandahållas.

5.8 Återkallande av samtycke

Den registrerade kan när som helst återkalla sitt samtycke varefter behandling inte längre får ske.

Det är viktigt att vi har en rutin för att kunna glömma en användare. Det innebär att vissa uppgifter raderas medan andra anonymiseras. Idag kan detta endast göras manuellt.

5.9 Fall där samtycke inte krävs

I några fall krävs inte samtycke enligt artikel 6 i dataskyddsförordningen. Detta gäller för nödvändigbehandling för att:

Avtal med den registrerade ska kunna fullgöras eller åtgärder som den registrerade begärt ska kunna vidtas innan ett avtal träffas.

Personuppgiftsansvarige ska kunna fullgöra en rättslig förpliktelse (lag, kollektivavtal etc).

Skydda vitala intressen för den registrerade.

Vid intresseavvägning (gäller ej känsliga personuppgifter). Se förklaring i bilaga.

Vi ser inte att ovanstående är tillämpligt, dvs. vi har inga skäl att behandla personinformation utan samtycke.

5.10 Otillåten behandling

Särskilda regler gäller för känsliga personuppgifter. Enligt artikel 9 i GDPR är det inte tillåtet att behandla känsliga personuppgifter såvida den inte är absolut nödvändig eller samtycke inhämtats. Känsliga personuppgifter är uppgifter som avslöjar:

Ras eller etniskt ursprung

Politiska åsikter

Religiösa eller filosofiska övertygelser

Medlemskap i fackförening

Uppgifter som rör sexualitet och hälsa

Genetiska och biometriska uppgifter.

Vi behandlar inga känsliga personuppgifter. I teorin skulle användargenererad information innehålla känsliga personuppgifter. **Vi kan skriva i avtalet som användaren godkänner att det förutsätts att inga känsliga personuppgifter enligt ovan lämnas. Vi behöver också ha som rutin när en hjärtstartare kontrolleras att uppgifterna kontrolleras och onödiga personuppgifter eller känslig information tas bort.**

5.11 Behandlas personuppgifterna på ett betryggande sätt?

Decerno har utarbetade rutiner och en IT-säkerhetspolicy som beskriver hur vi hanterar personuppgifter på ett säkert sätt. Utgångspunkten är att endast personer inom vår organisation som har behov av personuppgifterna för att utföra sina arbetsuppgifter ska ha tillgång till dem. För tillgång till känsliga personuppgifter krävs särskild behörighet. Vi har en god fysisk och elektronisk säkerhet kring de ställen vi lagrar personinformation på och vi överför inte personuppgifter från ett ställe till ett annat för andra ändamål än för de som anges i denna policy. Vi har rutiner för att upptäcka och rapportera intrång i enlighet med gällande dataskyddslagstiftning.

HLR-rådet behöver vid behov konsultera sin driftpartner EPM och från dem få motsvarande försäkran och policy. Detta sker lämpligen genom tecknande av personuppgiftsbiträdesavtal.

5.12 När lämnar vi ut personuppgifter?

SHR:s utgångspunkt är att endast lämna ut personuppgifter till tredje part om det är nödvändigt för att uppfylla våra förpliktelser enligt lag eller avtal eller om vi först fått samtycke till det. I fall som inte grundas på utlämnande enligt lag, upprättar HLR-rådet sekretessavtal med tredje part samt säkerställer att personuppgifterna hanteras och behandlas på ett betryggande sätt.

5.13 De registrerades rättigheter

De viktigaste rättigheterna för de registrerade är att:

Få veta vilken information vi sparat om personen, alltså inte uppgifterna som sådana.

- Vi kan lätt meddela en person vilka uppgifter som sparas om honom/henne.

Få felaktiga personuppgifter rättade

- Om en användare hör av sig och har felaktiga uppgifter kan HLR-rådet rätta uppgifterna, och vid behov kan Decerno bistå.

Få sina personuppgifter raderade (bli glömd)

- Det går idag inte att radera en persons uppgifter utan att radera alla hjärtstartare den personen har registrerade

Invända mot att personuppgifter används för automatiserat beslutsfattande och profilering

- **Inget automatiserat beslutsfattande eller profilering sker idag.**

Flytta de personuppgifter som den registrerade själv har lämnat till oss (dataportabilitet)

- **Detta är inte aktuellt. Det finns inga andra register som uppgifterna kan flyttas till.**

Dataskyddsförordningen innehåller en skyldighet att på begäran lämna information till de registrerade om vilka uppgifter som behandlas om dem. När en sådan begäran hanteras behöver man även lämna viss ytterligare information, som exempelvis hur länge personuppgifterna kommer att lagras och att man har rätt att få felaktiga uppgifter rättade. Om en sådan begäran görs elektroniskt ska den registrerade också kunna begära att få ut informationen elektroniskt.

Vi behöver upprätta en rutin för hur vi går tillväga och hur vi ska lämna ut information i detta fall.

6 Ansvar

HLR-rådet är personuppgiftsansvarig för alla personuppgifter som man äger, vilket innebär att rådet är ansvariga för hur personernas uppgifter lagras, hur de behandlas och att personernas rättigheter tas tillvara.

Decerno ansvarar för att säkerställa att egenutvecklade system som erbjuds kunder, har sådana funktioner att våra kunder kan efterleva kraven på behandling av personuppgifter.

För personuppgifter som ägs av kund är denne personuppgiftsansvarig. I de fall Decerno behandlar personuppgifter för kunds räkning tecknas personuppgiftsbiträdesavtal som reglerar hur hantering av dessa ska ske mellan parterna.

6.1 Registerförteckning

Dokumentation över registrets behandling av personuppgifter ska sammanställas i en registerförteckning. Även ostrukturerat material ska ingå i denna förteckning.

En registerförteckning ska skapas för registret.

6.2 Samtycke

När Decerno inte har tillåtelse att inhämta eller behandla vissa personuppgifter, ska ett samtycke inhämtas.

Samtycke inhämtas idag för användarens personuppgifter. Samtycke för information om hjärtstartare behöver inhämtas.

6.3 Konsekvensbedömning

Innan man inleder en behandling av personuppgifter som kan leda till en hög risk för integritetsintrång, det kan till exempel vara ett omfattande register med känsliga personuppgifter, så måste man bedöma konsekvenserna för de registrerade. Det kallas för en konsekvensbedömning. Då bedömer man risken och allvaret om uppgifter skulle spridas. Resultatet av bedömningen avgör vilka åtgärder som behöver genomföras. Åtgärder behöver planeras och införas för att hantera riskerna, såsom skyddsåtgärder, säkerhetsåtgärder och rutiner för att säkerställa skyddet av personuppgifterna i förhållande till genomförandekostnaderna. Om man bedömer att behandlingen skulle leda till en hög risk om inte den personuppgiftsansvarige vidtar dessa åtgärder för att minska risken, måste man samråda med tillsynsmyndigheten.

De viktigaste principerna är att inte samla in mer information än vad som är nödvändigt, inte ha kvar informationen längre än nödvändigt samt att inte använda uppgifterna till annat än till angivet syfte. Beakta möjligheten att minimera tillgång till uppgifterna.

Denna utredning kan sägas vara en konsekvensutredning. Utredningen visar att det inte finns någon hög risk med lagringen av personuppgifter i SHR.

6.4 Personuppgiftsbiträdesavtal

Som personuppgiftsansvariga ska Decerno alltid teckna personuppgiftsbiträdesavtal med underleverantör när hantering av personuppgifter är aktuellt. Detta gäller såväl behandling av våra personuppgifter som i de fall underleverantör behandlar personuppgifter åt våra kunder.

Decerno ska även teckna personuppgiftsbiträdesavtal med sina kunder i de fall behandling av personuppgifter ska utföras åt kunden.

Personuppgiftsbiträdesavtal bör tecknas mellan HLR-rådet och Decerno. Decerno har mallar för sådana.

HLR-rådet bör även se till att sådant avtal tecknas med EPM.

6.5 Personuppgiftsincident

Om det inträffar en oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som Decerno behandlar, till exempel ett dataintrång (någon obehörig får access till vårt system) eller en oavsiktlig förlust av personuppgifter (en anställd tappar sin mobil, dator eller minnessticka), kan vi behöva dokumentera incidenten och anmäla den till tillsynsmyndigheten inom 72 timmar. Det behöver inte göras om det är osannolikt att incidenten leder till några risker för enskildas fri- och rättigheter (den förlorade datorn innehöll få eller inga personuppgifter eller innehållet var krypterat och datorn försedd med andra säkerhetsskydd). Vi kan också behöva informera de registrerade om det till exempel finns risk för id-stöld eller bedrägeri.

Vi bör upprätta en rutin för personuppgiftsincidenter.

DECERNO
ADDNODE GROUP

7 BILAGA 1: VANLIGA BEGREPP

Personuppgifter: Varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbar fysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller onlineidentifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Känsliga personuppgifter: Känsliga personuppgifter är uppgifter som avslöjar, ras eller etniskt ursprung, politiska åsikter, religiösa eller filosofiska övertygelser, medlemskap i fackförening, uppgifter som rör sexualitet och hälsa samt genetiska och biometriska uppgifter.

Behandling: En åtgärd eller kombination av åtgärder beträffande personuppgifter eller uppsättningar av personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring.

Intresseavvägningen innebär att det måste finnas ett berättigat intresse för den personuppgiftsansvarige som väger tyngre än den registrerades intresse av skydd mot kränkningar av den personliga integriteten. Det kan till exempel handla om att samla in personuppgifter genom cookies för att förbättra användarens upplevelse av webbplatsen eller förenkla inloggningen, liksom att skicka ut marknadsföringsinformation till en befintlig kunds e-postadress. Användning av de kategorierna av personuppgifter (cookies respektive e-postadress) anses innebära en låg risk för kränkning om ändamålet är relativt harmlöst.

Profilering: Varje form av automatisk behandling av personuppgifter som består i att dessa personuppgifter används för att bedöma vissa personliga egenskaper hos en fysisk person, i synnerhet för att analysera eller förutsäga denna fysiska persons arbetsprestationer, ekonomiska situation, hälsa, personliga preferenser, intressen, pålitlighet, beteende, vistelseort eller förflyttningar.

Pseudonymisering: Behandling av personuppgifter på ett sätt som innebär att personuppgifterna inte längre kan tillskrivas en specifik registrerad utan att kompletterande uppgifter används, under förutsättning att dessa kompletterande uppgifter förvaras separat och är föremål för tekniska och organisatoriska åtgärder som säkerställer att personuppgifterna inte tillskrivs en identifierad eller identifierbar fysisk person.

Register: En strukturerad samling av personuppgifter som är tillgänglig enligt särskilda kriterier, oavsett om samlingen är centraliserad, decentraliserad eller spridd på grundval av funktionella eller geografiska förhållanden.

Registerutdrag: Omfattar uppgifter som vilka personuppgifter som behandlas, för vilket ändamål, hur länge de lagras samt till vem eller vilka de lämnats ut.

Personuppgiftsansvarig: En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter; om ändamålen och medlen för behandlingen bestäms av unionsrätten eller medlemsstaternas nationella rätt kan den personuppgiftsansvarige eller de särskilda kriterierna för hur denne ska utses föreskrivas i unionsrätten eller i medlemsstaternas nationella rätt.

Personuppgiftsbiträde: En fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som behandlar personuppgifter för den personuppgiftsansvariges räkning.

Samtycke av den registrerade: varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne.

Personuppgiftsincident: En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats. Andra exempel på personuppgiftsincidenter kan t.ex. vara:

En besökare har använt skrivaren och lämnat utskrifter kvar i skrivaren som innehåller kundlistor med kontaktuppgifter

En anställd råkar ta bort information i en databas som innehåller personuppgifter

Ett mail som innehåller personuppgifter skickas till fel mottagare utanför organisationen

8 Bilaga 2: Villkor för registrering av användare

Här finner du avtalsvillkoren för registrering av användare på Sveriges Hjärtstartarregister, hädanefter kallat SHR. Villkoren kan komma att uppdateras och de nya villkoren presenteras då på hjartstartarregistret.se. Ändringar i villkoren blir gällande mot dig som registrerad 30 dagar efter det att de nya villkoren publicerats på hjartstartarregistret.se, om du inte meddelar oss skriftligen inom dessa 30 dagar att du motsätter dig uppdateringen. Ett sådant meddelande har samma verkan som att användaren (inklusive registrerade hjärtstartare) tas bort – glöms – av registret, om vi inte kommer överens om någonting annat.

8.1 Om Sveriges Hjärtstartarregister

HLR-rådet, 802425-6417, driver SHR. Du kan nå oss via epost till info@hjartstartarregistret.se.

Ytterligare kontaktinformation kan i framtiden stå att finna på vår webbplats hjartstartarregistret.se.

8.2 Behandling av personuppgifter

Genom att godkänna det här avtalet ger du ditt medgivande till att SHR sparar och behandlar de personuppgifter som du lämnar till oss när du registrerat dig som användare, i syfte att göra hjärtstartare synliga på kartan för att rädda fler liv.

SHR lagrar bara nödvändig information. Om en användare inte har någon hjärtstartare registrerad glöms användaren av SHR, dvs. alla personuppgifter tas bort, efter en viss tid, som beslutas av HLR-rådet, dock längst ett år.

SHR lämnar inte ut personuppgifter som lämnats vid registrering av användare till tredje part.

8.2.1 Information, rättelse eller avslutning

Om du vill veta vilken typ av information som finns lagrad i registret om dig som person, vill ha rättelse av felaktig information eller vill bli glömd av SHR, kontakta SHR via info@hjartstartarregistret.se

8.3 Användning av SHR

För att ta del av våra tjänster förutsätts att du har teknisk utrustning för att kunna ta del av webbplatsen hjartstatarregistret.se på ett tillfredsställande sätt. Det kan vara genom dator, surfplatta eller mobiltelefon med internetuppkoppling. Du behöver också ha tillgång till de versioner av programvara som stödjer vår tjänst.

DECERNO
ADDNODE GROUP

9 Bilaga 3: Villkor för registrering av hjärtstartare

Här finner du avtalsvillkoren för registrering av hjärtstartare på Sveriges Hjärtstartarregister, hädanefter kallat SHR. Villkoren kan komma att uppdateras och de nya villkoren presenteras då på hjartstartarregistret.se. Ändringar i villkoren blir gällande mot dig som registrerad 30 dagar efter det att de nya villkoren publicerats på hjartstartarregistret.se, om du inte meddelar oss skriftligen inom dessa 30 dagar att du motsätter dig uppdateringen. Ett sådant meddelande har samma verkan som att användaren (inklusive registrerade hjärtstartare) tas bort, glöms av registret, om vi inte kommer överens om någonting annat.

9.1 Om Sveriges Hjärtstartarregister

HLR-rådet, 802425-6417, driver SHR. Du kan nå oss via epost till info@hjartstartarregistret.se.

Ytterligare kontaktinformation kan i framtiden stå att finna på vår webbplats hjartstartarregistret.se

9.2 Behandling av personuppgifter

Du uppmanas att i största möjliga utsträckning avstå från att mata in personuppgifter som inte är nödvändiga i den information du delar, eftersom informationen kommer att göras tillgänglig på kartan och för samarbetspartners enligt nedan.

Genom att godkänna det här avtalet ger du ditt medgivande till att SHR sparar och behandlar de uppgifter som du lämnar till oss, i syfte att göra hjärtstartare synliga på kartan för att rädda fler liv. All information om hjärtstartaren kan komma att presenteras för allmänheten på kartan, om du inte valt att dölja din hjärtstartare på kartan. Om du väljer att dölja din hjärtstartare på kartan kommer uppgifterna inte att synas för allmänheten på våra kartor.

Du ger även ditt medgivande till att HLR-rådet låter SOS Alarm samt mobila livräddare få tillgång till all information om din hjärtstartare, även om du valt att dölja den på kartan. Detta i syfte att snabbt få en hjärtstartare till en person med hjärtstopp och rädda liv.

Du ger även ditt medgivande till att övriga samarbetspartners, t.ex. kommuner, får tillgång till all information om din hjärtstartare, om du inte valt att dölja din hjärtstartare på kartan. Om du väljer att dölja din hjärtstartare på kartan kommer dessa samarbetspartners inte att få information om din hjärtstartare. Samarbetspartners får informationen om din hjärtstartare för att presentera informationen i sina tjänster, som också syftar till att presentera hjärtstartare på kartan och rädda fler liv.

Du ger även ditt medgivande till att HLR-rådet bedriver registerforskning om hjärtstartares placering och användning, baserat på anonymiserad information om hjärtstartare. HLR-rådet kan också lämna ut anonymiserad information om hjärtstartare till forskningsinstitutioner i syfte att bedriva registerforskning om hjärtstartares placering och användning.

HLR-rådet ställer som villkor att du som användare inte matar in någon information om hjärtstartaren som kan klassas som känslig information, vilket inkluderar:

- Ras eller etniskt ursprung
- Politiska åsikter
- Religiösa eller filosofiska övertygelser
- Medlemskap i fackförening
- Uppgifter som rör sexualitet och hälsa
- Genetiska och biometriska uppgifter.

SHR lagrar bara nödvändig information. Om en hjärtstartare ej längre är validerad i systemet eller är borttagen, kommer all information, t.ex. innehavare, att anonymiseras efter en viss tid, som bestäms av HLR-rådet, dock längst ett år.

9.2.1 Information, rättelse eller avslutning

Om du vill veta vilken typ av information som finns lagrad i registret om dig som person, vill ha rättelse av felaktig information eller vill bli glömd av SHR, kontakta SHR via info@hjartstartarregistret.se

9.3 Användning av SHR

För att ta del av våra tjänster förutsätts att du har teknisk utrustning för att kunna ta del av webbplatsen hjartstatarregistret.se på ett tillfredsställande sätt. Det kan vara genom dator, surfplatta eller mobiltelefon med internetuppkoppling. Du behöver också ha tillgång till de versioner av programvara som stödjer vår tjänst.