Säkerhetsbeskrivning Vårdbetyg

Version 1.1, 31 oktober 2026

Gäller Min mottagning, Insikt och Patientpuls, enkäten som en vårdcentral kan skicka till sina egna patienter. Dokumentet beskriver bara det som gäller vid datumet ovan. Det vi inte har står i avsnitt 10. Den senaste versionen finns på vardbetyg.se/for-vardgivare/sakerhet.

1. Leverantören

Vårdbetyg drivs som enskild firma av grundaren Arvid Pilhall, som också är personuppgiftsansvarig för vardbetyg.se. Frågor om säkerhet och dataskydd mejlas till hej@vardbetyg.se. Dit skickar man också en rapport om en säkerhetsbrist, och adressen står i vardbetyg.se/.well-known/security.txt enligt standarden RFC 9116.

2. Var uppgifterna lagras

Del	Tjänst	Plats
Server	Firebase App Hosting och Cloud Run	Googles region europe-west4, Nederländerna
Databas	Cloud SQL med PostgreSQL	europe-west4, Nederländerna
Serverlogg	Cloud Logging	europe-west4 sedan 30 oktober 2026
Googles granskningslogg över ändringar i projektet	Cloud Logging	Googles globala region, 400 dagar

Rader i serverloggen från tiden före 30 oktober 2026 ligger kvar i Googles globala region tills de raderas efter 30 dagar, alltså senast 29 november 2026. Granskningsloggen innehåller inga anrop från besökare eller patienter, bara ändringar i driftmiljön.

Anropen tas emot i Googles nätverk, och Googles CDN kan spara kopior av sajtens offentliga sidor närmare besökaren. Enkäten och inloggningen sparas aldrig där.

3. Kryptering

- Trafiken mellan webbläsaren och oss går alltid över HTTPS. Anrop till http:// skickas vidare till https://.
- Webbläsaren får besked (HSTS) att i två år bara ansluta krypterat, även till underdomäner.
- Certifikatet kommer från Google Trust Services och förnyas automatiskt.
- Allt som lagras, alltså databasen, servrarnas diskar och loggarna, krypteras med Googles standardkryptering och nycklar som Google hanterar.
- Sidorna skickar säkerhetsrubriker som hindrar andra webbplatser från att bädda in dem och begränsar vilka skript som får köras.

4. Vad Patientpuls sparar

Vårdcentralen skickar själv länken till enkäten i ett SMS, på ett kvitto eller med en QR-kod i väntrummet. Samma länk går till alla. Enkäten har sex frågor och tre frivilliga tillvalsfrågor om bemötande, delaktighet och information, alltså upp till nio. Vårdcentralen väljer vilka av dem en länk ställer.

- Ett svar sparas aldrig som en egen rad. Det räknas direkt in i summor per vårdcentral, månad, fråga och svarsalternativ.
- Ingen IP-adress, ingen uppgift om webbläsaren och ingen tid finare än månaden sparas med svaren.

- Formuläret har bara fasta svarsalternativ och inga fritextfält. Ett svar med ett okänt fält avvisas helt.
- Formuläret sparar inget i webbläsaren, varken kakor eller annat. Det har ingen besöksmätning och inga skript från andra företag.
- Vi tar aldrig emot namn, personnummer, telefonnummer eller mottagarlistor.
- Länkens kod står efter tecknet # i adressen, och det gör också vårdcentralens korta namn i den korta länken (vardbetyg.se/puls#abrahamsberg). Den delen skickar webbläsaren aldrig till servern, så serverloggen ser inte vilken vårdcentral ett svar gäller. Formuläret skickar koden eller namnet i själva meddelandet.
- Svarsmönster och räkning per dygn, som behövs för att upptäcka om någon fyller i många gånger, raderas när månaden är slut. Månadssummorna raderas efter 24 månader.
- Ett provsvar, när vårdcentralen själv testar enkäten med Testa själv i Min mottagning, räknas aldrig. I en egen tabell (patientpuls_prov) sparas bara vårdcentralen och klockslaget då dess senaste provsvar kom fram, aldrig något om svaret. Raden raderas efter 24 timmar.
- Svaren visas aldrig offentligt, påverkar aldrig vårdcentralens betyg och finns aldrig i våra öppna data. Ett automatiskt test stoppar varje ändring som skulle låta sajtens offentliga sidor, betygsberäkningen eller exporten läsa enkätens tabeller.

5. Vad vårdcentralen ser

Resultatet visas bara i vårdcentralens inloggning i Min mottagning, och bara för månader som är slut. Under en pågående månad visas bara hur många som har svarat hittills.

En månad visas först när minst 10 personer har svarat, och varje fråga först när minst 10 har svarat på just den frågan. Andelarna avrundas till hela 5 procentenheter, och en grupp med ett eller två svar visas som "färre än 3" utan siffra. En avslutad månad ändras aldrig i efterhand, så det går inte att räkna fram ett enskilt svar genom att jämföra före och efter.

6. Åtkomst

Vårdcentralens inloggning. Kontona i Min mottagning är personliga och skapas bara på inbjudan från oss. Aktiveringslänken gäller i 72 timmar. Lösenordet ska ha minst 10 tecken och sparas bara som en scrypt-hash med ett eget salt, aldrig i klartext. Inloggningen bärs sedan av en signerad sessionskaka som skript på sidan inte kan läsa och som bara skickas krypterat. Den slutar gälla efter 7 dagar utan besök och senast 14 dagar efter inloggningen, även om den används hela tiden. Ingen IP-adress sparas för inloggningen.

Varje session kontrolleras mot kontot vid varje sidvisning. I Min mottagning finns knappen Logga ut från alla enheter, som gör att alla inloggningar med kontot slutar gälla direkt, i alla webbläsare. Detsamma händer när man får en ny aktiveringslänk och väljer ett nytt lösenord.

Misslyckade inloggningar räknas, och efter för många försök under samma timme stoppas alla inloggningar innan lösenordet ens prövas. Svaret är detsamma för fel adress och fel lösenord, så det går inte att ta reda på vilka konton som finns.

En inloggning når bara den egna vårdcentralens uppgifter. Vilken vårdcentral det gäller läses alltid ur den signerade sessionen, aldrig ur det som webbläsaren skickar. Min mottagning och enkäten sparas inte i någon cache, indexeras inte av sökmotorer och laddar inga skript från andra företag.

Hos oss. Grundarens konto är det enda personliga kontot i Googles driftmiljö. De andra kontona där är tjänstekonton som kör sajten. Databasen tar inte emot direkta anslutningar från internet, bara via Googles egen anslutning för Cloud SQL med ett behörigt konto. Det finns ingen intern vy där vi läser vårdcentralernas enkätresultat. Grundaren kan som driftansvarig nå databasen, men där finns bara summorna.

Grundaren har dessutom en administratörsinloggning till Min mottagning, med lösenord och en engångskod från en app i telefonen (tvåstegsverifiering), som gäller en timme i taget. Där kan han se Min mottagning som en viss

vårdcentral ser den, men aldrig Patientpuls, och ingenting kan ändras därifrån. Varje sådan visning skrivs i en logg med vem, vilken vårdcentral och när.

7. Loggar

Googles plattform sparar varje anrop till sajten i en serverlogg med IP-adress, webbläsarens identifiering, adressen, adressen besökaren kom ifrån och tidpunkten. Loggen raderas automatiskt efter 30 dagar. För enkäten står bara adressen /puls i loggen, samma för alla vårdcentraler. Vi använder loggen för drift och säkerhet och för att räkna sammanlagda besök per sida, aldrig för att följa en enskild person.

8. Underbiträden och andra leverantörer

Leverantör	Vad	Patientpuls
Google (Google Cloud EMEA Limited enligt Googles villkor för kunder i EES)	Server, databas och logg i EU: Firebase App Hosting, Cloud Run, Cloud SQL, Cloud Logging	Enda underbiträdet
Cloudflare	Bara namnuppslagning (DNS) för vardbetyg.se. Besöksmätning och robotskydd på sajtens offentliga sidor	Ser inte trafiken till enkäten eller Min mottagning
Resend	Aktiveringsmejlet när vi skapar ett konto: mottagarens adress och länken	Nej
Anthropic	AI-analysen i Insikt: vårdcentralens öppna siffror och summor av besöken på dess sida hos oss	Nej. Aldrig enkätsvar, åtgärder, anteckningar eller kontouppgifter

Googles villkor för personuppgiftsbehandling i molntjänsterna gäller. Vi meddelar vårdcentralen 30 dagar innan ett underbiträde för Patientpuls byts eller läggs till.

Överföring utanför EU. Uppgifterna lagras i EU, men Google är ett amerikanskt företag. Google kan därför i vissa fall behandla uppgifter utanför EU, till exempel vid support och felsökning, och amerikansk lag kan ge myndigheter där rätt att begära ut uppgifter från amerikanska företag. Sådana överföringar har stöd i EU-kommissionens beslut om EU-US Data Privacy Framework, där Google LLC är certifierat, och i EU:s standardavtalsklausuler i Googles villkor. För Patientpuls gäller frågan i praktiken serverloggen, eftersom databasen bara har summor. Resend och Anthropic finns i USA. Till Anthropic går inga personuppgifter, och till Resend bara mottagarens e-postadress i aktiveringsmejlet.

9. Avtal och incidenter

För Patientpuls är vårdcentralen personuppgiftsansvarig och Vårdbetyg personuppgiftsbiträde. Biträdesavtalet ingår i villkoren som vårdcentralen godkänner i Min mottagning innan den första länken skapas, och finns också som eget dokument. En region eller koncern kan använda sin egen mall i stället.

Upptäcker vi en personuppgiftsincident som rör vårdcentralen meddelar vi den inom 24 timmar, så att den hinner bedöma om incidenten ska anmälas till IMY. Detsamma gäller om patientuppgifter av misstag har hamnat i en länk eller i formuläret. Då raderar vi dem.

Vårdcentralen kan stoppa en enskild länk direkt i Min mottagning, och vi kan stänga av hela enkättjänsten för alla med en inställning. Sajten kontrolleras varje minut från flera platser, och vi får ett larm om den slutar svara.

10. Det här har vi inte i dag

- Ingen certifiering för informationssäkerhet.
- Inga kundstyrda nycklar. Lagrad data krypteras med Googles nycklar.

- Ingen tvåstegsverifiering i vårdcentralernas inloggning till Min mottagning.

Fråga oss gärna om något av det betyder något för er upphandling.

Vårdbetyg, hej@vardbetyg.se. Senaste versionen finns på vardbetyg.se/for-vardgivare/sakerhet.