Wetenschappelijk Onderzoek- en Documentatiecentrum

Cahier 2021-2

Dataveiligheid en privacy bij het gebruik van fysiologische wearables in de justitiële context

Een casusonderzoek met de Empatica E4

S.W. van den Braak
E. Platje
C.H. de Kogel

Cahier
De reeks Cahier omvat de rapporten van onderzoek dat door en in opdracht van het WODC is verricht. Opname in de reeks betekent niet dat de inhoud van de rapporten het standpunt van de Minister van Justitie en Veiligheid weergeeft.

Dankwoord

Fysiologische wearables hebben de potentie om behandeling te personaliseren, veiligheid in detentie te verbeteren, reclasseringstoezicht te verrijken en zelfredzaamheid van justitiabelen te vergroten, zo laat eerder verkennend WODC-onderzoek zien (Cornet et al., 2017; De Kogel, 2019). Er zijn echter ook serieuze aandachtspunten en risico's verbonden aan het gebruik van technologische zelfmeetmethoden. Uit het verkennend onderzoek en uit gesprekken met ervaringsdeskundigen blijkt bijvoorbeeld dat er zorgen zijn rondom de veiligheid van de opslag en het beheer van gegevens verzameld met technologische zelfmeetmethoden. Dat is de reden dat het WODC het onderhavige casusonderzoek heeft uitgevoerd. Voor u ligt het resultaat: het rapport 'Dataveiligheid en privacy bij het gebruik van fysiologische wearables in de justitiële context; Een casusonderzoek met de Empatica E4'.

Aan de totstandkoming van het rapport hebben verschillende mensen bijgedragen. Graag willen wij de leescommissie bestaande uit Ton Eijken, Ernst Eilering, Erik Leertouwer, Peter de Looff, Matthijs Noordzij en Stefania Rosanio, danken voor hun waardevolle en constructieve bijdragen. Matthijs Noordzij en Peter de Looff zijn pioniers op het gebied van de inzet van fysiologische wearables in de justitiële context en hebben daarover een enorme kennis. Erik Leertouwer heeft vanuit zijn rol als Privacy Officer bij het WODC scherp gekeken naar de consequenties van gegevensverzameling met fysiologische wearables voor de privacy van justitiabelen. Hij heeft ons daartoe ook relevante bronnen aangereikt en heeft daarbij ook Chief Information Officer Ted Mos van de Dienst Justitiële Inrichtingen geconsulteerd. Ton Eijken, Ernst Eilering en Stefania Rosanio hebben het WODC gevraagd om dit project uit te voeren. Vanuit hun rol bij beleidsdirectie of uitvoeringsorganisatie van het ministerie van Justitie en Veiligheid, geven zij aan de nieuwe mogelijkheden van fysiologische wearables bij onder meer de behandeling en het toezicht ten aanzien van justitiabelen op een verantwoorde manier te willen benutten. Oud-WODC-collega Liza Cornet danken we voor het maken van een start met dit casusonderzoek. WODC-collega Mortaza S. Bargh heeft met ons meegedacht over de betekenis van 'big data', zoals die met fysiologische wearables kunnen worden verzameld, voor de identificeerbaarheid van personen, en dat was een eyeopener. Tot slot heeft het deskundige commentaar van jurist Suzanne Hartholt van de Directie Inkoop en Informatievoorziening van het ministerie van JenV een waardevolle bijdrage geleverd waarvoor wij haar graag bedanken.

De auteurs

Inhoud

Samenvatting

Aanleiding en onderzoeksvragen

Onderzoek laat zien dat technologische zelfmeetmethoden de potentie hebben om behandeling te personaliseren, veiligheid in detentie te verbeteren, reclasseringstoezicht te verrijken en zelfredzaamheid van justitiabelen te vergroten. Niettemin zijn er ook serieuze aandachtspunten en risico's verbonden aan het gebruik van technologische zelfmeetmethoden. Zo is het vaak onduidelijk wat er precies met gegevens gebeurt nadat deze verzameld zijn. Gegevens die verzameld worden met technologische zelfmeetmethoden, zijn veelal ook toegankelijk voor de fabrikant en worden mogelijk gedeeld met derden. Ook is de technologie soms kwetsbaar voor het onderscheppen of stelen van gegevens door derden. Dit is zeker in de justitiële context – waarin veiligheid en privacybescherming voorop staat – niet wenselijk. Voordat technologische zelfmeetmethoden op grotere schaal in de justitiële context gebruikt kunnen worden, is het daarom van belang te onderzoeken hoe het gesteld is met de dataveiligheid bij dergelijke methoden en wat binnen de justitiële context eventueel zou kunnen worden gedaan om de veiligheid van verzamelde gegevens en daarmee de privacy van de betrokkenen te waarborgen.

In dit rapport beschrijven we een casusonderzoek hiernaar waarbij we ons specifiek gericht hebben op *fysiologische wearables*. Dit zijn draagbare apparaatjes die om de pols of op het lichaam gedragen worden en waarmee door middel van sensoren fysiologische gegevens verzameld kunnen worden. Dit casusonderzoek is verricht aan de hand van één specifieke wearable: de Empatica E4.

De volgende deelvragen staan centraal:
1 Wat gebeurt er met de fysiologische gegevens van de Empatica E4 nadat deze verzameld zijn door de gebruiker met betrekking tot: gegevensopslag, gegevenstransport en toegang tot de gegevens door derden?
2 Wat zijn de risico's daarbij voor de veiligheid van de gegevens en voor de privacy van de drager? En hoe zien de risico's en de geboden functionaliteit eruit in vergelijking met andere wearables?
3 Welke kennis, ervaringen en zorgen hebben professionele gebruikers van de Empatica E4 met betrekking tot gegevensopslag, toegang tot gegevens door derden en privacy?
4 Wat betekenen de antwoorden op de deelvragen voor het gebruik van de Empatica E4 en andere fysiologische wearables in de justitiële context?

Op basis van het casusonderzoek worden aanbevelingen gedaan over hoe in de justitiële context het beste omgegaan zou kunnen worden met de veiligheid en privacy van gegevens zoals die worden verzameld met fysiologische wearables. *Veiligheid* van de gegevens heeft betrekking op de beveiliging rondom gegevensopslag en -transport. Met *privacy* wordt in dit rapport bedoeld dat de verzamelde (persoons)gegevens van de drager beschermd worden om onthullingen te voorkomen.

In dit rapport wordt voornamelijk het gebruik van wearables voor onderzoek, behandeling of toezicht besproken. Daarbij onderscheiden we de *gebruiker* en de *drager*. De *gebruiker* (bijvoorbeeld een onderzoeker, behandelaar of toezichthouder) is degene die de gegevens verzamelt, opslaat, verwerkt, analyseert en eventueel

verwijdert. Veelal is de gebruiker ook degene die de wearable aanschaft, een overeenkomst met de fabrikant aangaat en zijn of haar persoonlijke gegevens verstrekt hiervoor. De *drager* is degene die de wearable draagt en van wie de fysiologische gegevens worden verzameld. Dit is bijvoorbeeld een justitiabele die deelneemt aan wetenschappelijk onderzoek of aan een pilot van behandelaars of toezichthouders.

Methoden en beperkingen

Deelvragen 1 en 2 zijn beantwoord door deskresearch uit te voeren. Er is naar informatie en documentatie over veiligheid en privacy gezocht op de website van Empatica en er zijn daarover aanvullende vragen aan Empatica gesteld. Ook is een account bij Empatica aangemaakt om de opslag, het transport en het gebruik van gegevens met de Empatica E4 in de praktijk uit te proberen. Voor de vergelijking van de dataveiligheid en privacy van de Empatica E4 met die van andere wearables (onderdeel van deelvraag 2), zijn relevante wearables gezocht door met systematische zoektermen verschillende internetbronnen te raadplegen en door experts te bevragen. Voor de analyse hebben we alleen de wearables geselecteerd die evenals de Empatica E4 huidgeleiding en/of hartslag kunnen meten en daarnaast idealiter ook beweging en/of huidtemperatuur. Deelvraag 3 is beantwoord door middel van een korte enquête onder tien professionele gebruikers van de Empatica E4 en deelvraag 4 is beantwoord op basis van de bevindingen wat betreft de eerste drie vragen.

In dit onderzoek is de Empatica E4 vergeleken met een aantal andere wearables. Hierbij hebben we enerzijds gekeken naar de geboden functionaliteit en anderzijds naar de dataveiligheid en privacy. Een belangrijke beperking is dat deze vergelijking niet uitputtend is. Wij hebben niet voor meerdere wearables alle risico's met betrekking tot dataveiligheid en privacy volledig in kaart kunnen brengen omdat wij de gegevens daarover hebben verzameld via openbare bronnen als websites. Deze bronnen omvatten wat dit betreft niet altijd alle details. Een beperking is daarnaast dat de gebruikerservaringen onderzocht zijn in een zeer kleine steekproef (mede doordat er in Nederland maar weinig gebruikers zijn). Ook heeft deze gebruikersraadpleging plaatsgevonden voordat de Algemene Verordening Gegevensbescherming (AVG) in werking trad en kan de kennis van de gebruikers inmiddels toegenomen zijn.

Dataveiligheid en privacy bij gebruik van de Empatica E4

De Empatica E4-polsband die vier verschillende sensoren bevat (huidgeleiding, hartslag, beweging en huidtemperatuur) kan op twee manier gebruikt worden. In de streamingmodus worden de gegevens van de polsband direct in real time in een app op een mobiel apparaat getoond. Deze gegevens worden vervolgens automatisch geüpload naar het *E4 Connect*-account van de gebruiker op de servers van Empatica. In de opnamemodus worden de gegevens die op de polsband zijn opgeslagen na verbinding met de computer automatisch verplaatst naar een opslaglocatie op de computer en vervolgens automatisch geüpload naar het account van de gebruiker. Op de *E4 Connect*-website kunnen de gegevens bekeken worden.

Een dergelijke omgeving waarin gegevens niet lokaal bij de gebruiker, maar op de servers van een derde partij worden opgeslagen, wordt ook wel een cloud of cloudomgeving genoemd. De gegevens in de cloud zijn vanaf ieder apparaat met een internetverbinding toegankelijk. Empatica biedt met *E4 Connect* niet alleen gegevensopslag, maar ook een website aan (ook wel een dashboard genoemd), waarmee de gegevens bekeken en beheerd kunnen worden.

Ons casusonderzoek laat zien dat Empatica verschillende maatregelen heeft genomen om de fysiologische gegevens van de dragers tijdens transport en opslag op de servers van Empatica te beveiligen tegen het eventuele onderscheppen ervan door derden. Zo worden de gegevens gekoppeld aan de gebruiker en niet aan de drager, opgeslagen in een speciaal formaat, en versleuteld verzonden. De fysiologische gegevens (van de drager van de polsband) zijn als gevolg hiervan alleen voor de gebruiker direct herleidbaar tot individuele personen en niet voor de fabrikant. Niettemin zien we verschillende risico's ten aanzien van de beveiliging van de verzamelde gegevens en ten aanzien van privacy van de drager.

Veiligheidsrisico's
Het belangrijkste veiligheidsrisico is dat de verzamelde fysiologische gegevens automatisch naar de online omgeving van de fabrikant gaan, lokaal (en offline) gebruik van de polsband is niet (gemakkelijk) mogelijk. Gegevens verzenden via internet en opslaan in de cloud brengt een groter risico met zich mee voor het digitaal onderscheppen of stelen van gegevens dan een oplossing die geheel offline werkt en gebruikmaakt van lokale opslag. In het geval van lokale offline opslag is dit moeilijker doordat er eerst fysieke toegang verkregen moet worden tot de opslag (terwijl de cloudopslag van afstand gehackt of aangevallen kan worden). Bij lokaal gebruik is er daarnaast voor de gebruiker meer flexibiliteit en controle over bijvoorbeeld waar de verzamelde gegevens opgeslagen worden, en gegevens van dragers worden dan niet (automatisch) met een externe partij gedeeld. De gebruiker is dan wel zelf verantwoordelijk voor afdoende beveiliging van de apparaten waarop de gegevens worden opgeslagen en geanalyseerd.

Privacyrisico's
Omdat de verzamelde fysiologische gegevens iets over iemands gezondheid kunnen zeggen, is er sprake van bijzondere persoonsgegevens die extra zijn beschermd. Met deze gegevens moet daarom zorgvuldig omgegaan worden, conform de op het gebruik van toepassing zijnde (privacy)wetgeving, om de privacy van de drager niet te schaden. Omdat bij de Empatica E4 gebruik wordt gemaakt van een cloudomgeving, waarbij Empatica de verwerker van de gegevens wordt, is het van belang om door een (privacy) jurist een goede verwerkersovereenkomst met Empatica te laten afsluiten. Dit is verplicht om aan de privacywetgeving te voldoen. Empatica heeft bij navraag van onze kant ook aangegeven bereid te zijn dergelijke overeenkomsten af te sluiten, en dat maatwerk mogelijk is. In de overeenkomst zou onder meer moeten worden afgesproken in welk land de gegevens worden opgeslagen, wie er toegang tot de gegevens krijgt en hoe lang deze bewaard worden. Voor gebruik in de justitiële context zou het bijvoorbeeld te allen tijde mogelijk moeten zijn om alle fysiologische gegevens van justitiabelen volledig en permanent te laten wissen.

Vergelijking dataveiligheid, privacy en functionaliteit van de Empatica E4 met andere fysiologische wearables

Diverse fabrikanten hebben wearables ontwikkeld voor gebruik door professionals in onderzoek of behandeling en daarnaast zijn er wearables op de consumentenmarkt beschikbaar die ook voor onderzoek, behandeling of toezicht zouden kunnen worden ingezet.

Wat opvalt als gekeken wordt naar *instrumenten die bedoeld zijn voor behandeling en onderzoek* is dat er grofweg twee varianten zijn: 1) wearables of draagbare apparaatjes voor gebruik in een lab of op een vaste locatie; en 2) wearables geschikt voor onderzoek op grotere schaal en/of behandeling op afstand, met veel verschillende deelnemers op verschillende locaties. Voor de eerste groep zijn er offlineoplossingen beschikbaar. Deze wearables bieden ook meer configuratiemogelijkheden voor de gebruikers, waarbij ze zelf kunnen bepalen welke metingen worden verzameld en waar deze worden opgeslagen. De gebruiker is er dan ook zelf verantwoordelijk voor maatregelen te nemen om de gegevens te beveiligen. Door de vele mogelijkheden lijken sommige van deze wearables wel meer technische expertise te vergen voor het gebruik. Bij de tweede groep wearables valt op dat alle aanbieders, net zoals Empatica, voor een cloudoplossing kiezen. Hierdoor is het voor de gebruikers gemakkelijker om grotere studies uit te voeren. Daarnaast is het deelnemen aan een studie voor de dragers laagdrempeliger: het is niet nodig om naar een lab te komen, de band kan langdurig thuis gedragen worden (sommige producten zijn zelfs waterdicht) en het kost weinig moeite om de metingen naar de gebruiker te sturen omdat dit grotendeels geautomatiseerd is. Bij sommige producten kunnen de dragers ook inzicht krijgen in hun eigen metingen door gebruik te maken van een mobiele app (geen van de producten heeft een scherm dat direct afleesbaar is).

Het gebruik van *consumenten wearables*, veelal smartwatches, voor onderzoek of behandeling is ook mogelijk. Dit heeft als voordeel dat de drager zelf de metingen in de gaten kan houden (door gebruik van het direct afleesbare scherm en/of gebruik van een app) en tegelijkertijd ook de andere functionaliteiten van de smartwatch kan gebruiken. Een nadeel voor gebruik van deze wearables in de justitiële context is dat deze instrumenten op dit moment nog (veel) minder sensoren hebben dan de producten gericht op professionals. Er zijn bijvoorbeeld nog niet veel smartwatches die huidgeleiding kunnen meten, maar veel smartwatches bevatten wel een hartslagsensor. Ook zijn de sensoren mogelijk niet altijd gevalideerd. Deze smartwatches maken over het algemeen gebruik van de cloud voor de opslag van de fysiologische gegevens.

Onze vergelijking laat zien dat er niet veel wearables op de markt zijn die net als de Empatica E4 een combinatie van meerdere verschillende fysiologische sensoren (zowel een hartslag- als een huidgeleidingssensor) bieden en daarnaast gemakkelijk bruikbaar zijn. Wel zijn er instrumenten die deze sensoren bevatten, maar daarbij gebruikmaken van (minder gebruiksvriendelijke) plakkers. Meerdere instrumenten scoren echter beter dan de Empatica E4 wat betreft: de mogelijkheid om het instrument volledig lokaal te gebruiken zonder dat de cloud nodig is of het bieden van een clouddienst met betere beveiligingsmaatregelen.

Ervaringen van professionele gebruikers

Hoewel een meerderheid van de gebruikers van de Empatica E4 vooraf de privacyverklaring heeft doorgenomen, heeft ook een derde van de gebruikers dat niet gedaan. Het is daardoor ook niet verwonderlijk dat bij veel van de vragen men neutraal antwoordt of niet weet hoe de fabrikant omgaat met gegevensopslag en -toegang. Bijna geen enkele gebruiker weet waar en hoe lang de verzamelde gegevens worden opgeslagen. Ook maakt men zich zorgen over toegang door derden en misbruik van gegevens. Gebruikers maken zich dus zorgen over de veiligheid van gegevensopslag en -toegang, maar gebruiken toch de wearable. Dit wordt wel de 'privacy paradox' genoemd en kan mogelijk verklaard worden doordat er weinig alternatieven voorhanden zijn.

Het gebruik van fysiologische wearables in de justitiële context

Op basis van ons casusonderzoek destilleren wij een aantal aspecten en aanbevelingen die van belang zijn voor het gebruik van fysiologische wearables in de justitiële context en meer specifiek het verzamelen van fysiologische gegevens bij justitiabelen.

Belangrijke opties voor fysiologische wearables in de justitiële context
Voor een wearable in de justitiële context zijn de volgende kenmerken van belang met het oog op dataveiligheid en privacy:

- mogelijkheid tot volledig lokaal gebruik; of,
- indien online gebruik (tevens) wenselijk is: adequate beveiligingsmogelijkheden en een verwerkersovereenkomst die voldoet aan de van toepassing zijnde privacywetgeving;
- mogelijkheid tot selectief aan en uitschakelen van individuele meetfuncties.

Daarnaast zijn de volgende kenmerken belangrijk met het oog op functionaliteit en gebruiksgemak (deels afhankelijk van de gewenste toepassing):

- een goed aanbod aan betrouwbare, valide en accurate meetfuncties bijvoorbeeld hartslag, huidgeleiding, beweging en (huid)temperatuur;
- voldoende draagcomfort zodat de wearable gemakkelijk geïntegreerd kan worden in het dagelijks leven;
- mogelijkheid tot een feedbackfunctie (bijvoorbeeld via een app op een ander mobiel apparaat of een schermpje op het device zelf).

De keuze voor een bepaald instrument en de geschiktheid ervan hangt samen met het precieze doel (bijvoorbeeld: welke meetfuncties nodig zijn, of directe feedback aan de drager via een schermpje nodig is enz.). Uit ons onderzoek komen twee varianten naar voren: een offline variant en een online variant. Welke variant de voorkeur verdient in de justitiële context, hangt af van het doel, de doelgroep en de specifieke context van het onderzoek, de behandeling of het toezicht. Een analyse van mogelijke risico's wat betreft dataveiligheid en privacy is daarbij van cruciaal belang.

Aanbevelingen
Op basis van het casusonderzoek hebben wij de volgende drie aanbevelingen.

1 *Stimuleer bewustzijn, maar ook verantwoord gedrag, wat betreft risico's voor dataveiligheid en privacy bij medewerkers die wearables gebruiken of ermee willen experimenteren.*
Benut de mogelijkheden van fysiologische wearables voor de behandeling en het toezicht ten aanzien van justitiabelen, maar faciliteer dat dit verantwoord gebeurt en zorg dat aan de van toepassing zijnde privacywetgeving wordt voldaan. Wettelijk gezien zijn de gebruikers als verwerkingsverantwoordelijke verplicht om de naleving van de privacywetgeving aan te tonen. Gebruikers van een wearable hebben met hun gedrag dan ook een belangrijke rol in het veilig omgaan met de verzamelde gegevens (bijvoorbeeld: gegevens beveiligen met een sterk wachtwoord, het zo snel mogelijk wissen van gegevens uit de cloudomgeving, niet meer aspecten meten dan noodzakelijk).

2 *Voer voorafgaand aan de keuze van een wearable een risicoanalyse uit ten aanzien van die wearable en pas de principes van privacy by design toe.*
De risicoanalyse vooraf zou zich moeten richten op de bovenvermelde punten van dataveiligheid en privacy. Het is aan te bevelen daarbij de Privacy Officer en/of Chief Information Security Officer te betrekken. Dit past ook bij het begrip *privacy by design*: al in een vroeg stadium aandacht besteden aan en rekening houden met privacy. In de justitiële context zou concreet de volgende werkwijze gevolgd moeten worden bij onderzoek, behandeling en toezicht met fysiologische wearables:
- *De gebruiker neemt passende technische en organisatorische maatregelen, volgt de principes van privacy by design, en kan als verwerkingsverantwoordelijke de naleving van de privacywetgeving aantonen, door onder andere:*
  - een verwerkingsregister bij te houden;
  - een *Data Protection Impact Assessment* (DPIA) uit te voeren;
  - een verwerkersovereenkomst met de verwerker af te sluiten (indien van toepassing).
- *Er wordt zorgvuldig omgegaan met de vaak kwetsbare doelgroep:*
  - binnen de doelgroep wordt gevraagd wie de wearable wil dragen (kan niet worden verplicht);
  - de drager wordt geïnformeerd over het doel van het onderzoek, de behandeling of het toezicht, over wat de consequenties zijn van dragen en wat er met de fysiologische gegevens gebeurt, zodat deze geïnformeerd en vrijelijk kan bepalen mee te doen;
  - toestemming van de drager wordt schriftelijk vastgelegd en kan te allen tijde weer worden ingetrokken.

3 *Investeer indien nodig in aanpassing van de software van een bestaande wearable zodanig dat deze voldoet aan de kenmerken die wenselijk zijn voor toepassing in de justitiële context.*
Er bestaan in Nederland verschillende praktijkvoorbeelden van onderzoeksprojecten waarbij de software van de wearables is aangepast. Een nadeel bij het aanpassen van een bestaande (commerciële) wearable kan zijn dat er nog steeds afhankelijkheid is van een commerciële derde partij. Dit kan financiële consequenties hebben. Ook is er een risico dat de productie stopt en dat er dan mogelijk geen ondersteuning en updates meer geboden worden, en het instrument veroudert of de beveiliging verslechtert. Om volledige regie te hebben over de functionaliteiten en om de aan veiligheids- en privacywaarborgen te voldoen zou het ministerie van Justitie en Veiligheid zelf kunnen investeren in het laten (door)ontwikkelen van een (bestaande) wearable.

1 Inleiding en methoden

1.1 Aanleiding tot het casusonderzoek

Vanuit het ministerie van Justitie en Veiligheid is er steeds meer interesse in het gebruik van technologische zelfmeetmethoden, zoals polsbandjes met biosensoren en mobiele apps. Die interesse geldt onder meer voor de nieuwe mogelijkheden die deze zogeheten *wearables* bieden om de begeleiding en behandeling van justitiabelen te versterken of verbeteren (zie voor een overzicht en concrete voorbeelden Cornet et al., 2017; De Kogel, 2019). Zo laat recent onderzoek zien dat met behulp van een polsband die huidgeleiding en hartslag meet, agressieve incidenten kunnen worden voorspeld (De Looff, 2019). Huidgeleiding verandert op basis van de activiteit van de zweetklieren in de huid en is een maat voor de activatie van het fysiologische stresssysteem. Potentieel belangrijk vanuit behandeloogpunt is dat met behulp van technologische zelfmeetmethoden de betrokkene ook zelf feedback kan ontvangen over de eigen fysiologische gegevens zoals hartslag of huidgeleiding (biofeedback). Zo zou betrokkene een seintje kunnen krijgen als de spanning oploopt. Dit schept nieuwe mogelijkheden voor een actievere rol in de eigen behandeling, bijvoorbeeld in het kader van agressieregulatie. Er wordt steeds meeronderzoek gedaan naar de bruikbaarheid van technologische zelfmeetmethoden voor begeleiding en behandeling binnen de justitiële context. Naast de kansen die dit biedt voor waardevolle vernieuwingen in onder meer behandeling en toezicht, is het belangrijk oog te hebben voor de mogelijke risico's van het gebruik ervan in de justitiële context. Daarom heeft het Directoraat-Generaal Straffen en Beschermen (DGSenB) het WODC gevraagd om dit casusonderzoek uit te voeren.

Deze technologische zelfmeetmethoden hebben deels dezelfde functionaliteit als instrumenten die voorheen enkel in een onderzoekssetting, bijvoorbeeld een laboratorium, bruikbaar waren. Tot voor kort moest men voor fysiologische metingen zoals hartslag of huidgeleiding 'bekabeld' op een plek blijven zitten verbonden met meetapparatuur,[1] of op zijn minst een kastje om het middel hangen met enkele sensoren die op de borst en rug geplakt werden.[2] Nu kan hartslag worden gemeten met draagbare sensoren die verwerkt zijn in een polsband of kledingstuk zoals een T-shirt. Eén van de voordelen is dat de metingen op die manier gemakkelijker in het dagelijks leven kunnen worden geïntegreerd.

Eerder verkennend onderzoek van het WODC laat zien dat technologische zelfmeetmethoden de potentie hebben om behandeling te personaliseren, veiligheid in detentie te verbeteren, reclasseringstoezicht te verrijken en zelfredzaamheid van justitiabelen te vergroten (Cornet et al., 2017; De Kogel, 2019). Hoewel het toepassen van technologische zelfmeetmethoden in de justitiële context in potentie zeker mogelijkheden biedt, zijn er ook serieuze aandachtspunten en risico's verbonden aan het gebruik van technologische zelfmeetmethoden. Uit het verkennend onderzoek en uit gesprekken met ervaringsdeskundigen blijkt dat er zorgen zijn rondom de veiligheid van de opslag en het beheer van gegevens verzameld met technologische zelfmeetmethoden. Zo is het vaak onduidelijk wat er precies met gegevens gebeurt nadat deze verzameld zijn. Gegevens die verzameld worden met

[1] Bijvoorbeeld BIOPAC een systeem voor fysiologische metingen en analyse in het laboratorium. www.biopac.com.

[2] Bijvoorbeeld het VU-AMS-systeem met ambulante meetapparatuur voor non-invasieve metingen aan het autonome zenuwstelsel (bijvoorbeeld hartslag en huidgeleiding) voor onderzoeksdoeleinden. www.vu-ams.nl.

technologische zelfmeetmethoden zijn veelal ook toegankelijk voor de fabrikant en deze worden mogelijk zelfs gedeeld met derden om winst te maken (Hengst et al., 2014; Cornet et al., 2017). Onduidelijkheid over de opslag en het beheer van gegevens is zeker in justitiële context – waarin veiligheid en privacybescherming voorop staat – niet wenselijk. Voordat technologische zelfmeetmethoden op grotere schaal in de justitiële context gebruikt kunnen worden, is het daarom van belang te onderzoeken hoe het gesteld is met de dataveiligheid bij dergelijke methoden en wat het ministerie van Justitie en Veiligheid eventueel zou kunnen doen om de veiligheid van verzamelde gegevens, en daarmee de privacy van de betrokkenen, te waarborgen. In dit rapport beschrijven we een eerste casusonderzoek hiernaar waarbij we ons specifiek gericht hebben op *fysiologische wearables*. Dit zijn draagbare apparaatjes (sensoren) die om de pols of op het lichaam gedragen worden en waarmee fysiologische en/of gezondheidsgegevens verzameld kunnen worden.

Om een indruk te krijgen van wat er met de verzamelde gegevens gebeurt, brengen we in dit rapport van één specifieke fysiologische wearable in kaart waar de verzamelde gegevens opgeslagen worden, wat er vervolgens mee gebeurt en wie er toegang toe heeft. Dit betreft de Empatica E4, een polsband met sensoren waarmee verschillende fysiologische gegevens kunnen worden verzameld. Er is voor de Empatica E4 gekozen omdat dit instrument reeds in proeftuinen binnen de justitiële context is gebruikt, evenals in enkele andere in de justitiële context relevante onderzoeken bij populaties met gedragsproblemen. Dienst Justitiële Inrichtingen (DJI) heeft voor zijn proeftuinen om meerdere redenen gekozen voor de Empatica E4. De eerste reden is dat de Empatica E4 op dat moment de enige wearable was die zowel hartslag als huidgeleiding en beweging kon meten. De tweede reden is dat de Empatica E4 draagvlak had bij collega-onderzoekers met betrekking tot de betrouwbaarheid van de metingen (in vergelijking tot een 'gouden standaard' als VU-AMS), in ieder geval onder rust-condities (Schuurmans et al., 2020; Van Lier et al., 2019). Een derde reden was dat de servers van de fabrikant Empatica waarop de gegevens worden bewaard, destijds in Europa (Italië) stonden. Dit zou een waarborg bieden voor het voldoen aan Europese privacyregelgeving.

De Empatica E4 is gebruikt in enkele voor het justitiële veld belangrijke onderzoeken naar fysiologische maten in relatie tot probleemgedrag. Zo heeft De Looff de Empatica E4 gebruikt in zijn onderzoek naar psychofysiologische maten (hartslag en huidgeleiding) als voorspellers van agressie bij sterk gedragsgestoorde licht verstandelijk beperkte cliënten en als voorspellers van burn-out symptomen bij hun begeleiders (De Looff, 2019).

Zowel DJI als DGSenB verkennen op dit moment de mogelijkheden van fysiologische wearables in de justitiële context. DJI heeft met de Empatica E4 geëxperimenteerd in het kader van twee proeftuinen: één in een forensisch psychiatrisch centrum en één in een penitentiaire inrichting (Rosanio, 2018). De eerste proeftuin 'Quantified Self' in Forensisch Psychiatrisch Centrum (FPC) de Oostvaarderskliniek is in 2017 afgerond. In deze pilot droegen terbeschikkinggestelden die wilden deelnemen enkele dagen tot weken de Empatica E4 polsband en konden zij een dagboekje bijhouden over hun ervaringen en emoties. De gegevens waren stof in de begeleidingsgesprekken van de terbeschikkinggestelde met zijn mentor, een sociotherapeut. Een tweede proeftuin in Justitieel Complex (JC) Zaanstad is in 2018 afgerond. In die proeftuin werd verkend of de Empatica E4 kon worden ingezet ter bevordering van bejegening en behandeling van gedetineerden. DJI acht fysiologische wearables en andere slimme meetapparatuur veelbelovend als een vernieuwend instrument binnen de bejegening en behandeling van justitiabelen (Rosanio, 2018).

DGSenB is betrokken bij een lopend onderzoek naar de mogelijkheid van biofeedback met draagbare meetapparatuur (polsband en app) bij jongeren met agressieproblematiek.

De behoefte leeft om binnen de justitiële context (meer) met dergelijke methoden te gaan werken. Dat is echter alleen haalbaar als de dataveiligheid en de privacybescherming niet tekortschieten. In het onderhavige rapport worden aan de hand van onze bevindingen met de Empatica E4 de dataveiligheid, en mogelijke risico's daarbij in het proces van opslag, transport, verwerking en beheer van gegevens, beschreven. Op basis van deze casus worden vervolgens voor zover mogelijk aanbevelingen gedaan over hoe in de justitiële context het beste omgegaan zou kunnen worden met fysiologische wearables en de veiligheid en privacy van gegevens zoals die worden verzameld met fysiologische wearables.

1.2 Risico's verbonden aan het gebruik van wearables

Het gebruik van moderne technologie, waaronder wearables, is niet zonder risico. Er kan hierbij het nodige misgaan, met mogelijk nadelige gevolgen voor de gebruiker, fabrikant en/of maatschappij. Dit illustreren we aan de hand van twee voorbeelden.

Op maandag 29 januari 2018 verschijnt het bericht in de media dat data van de fitness-app Strava geheime locaties van militairen toont.[3] Onderzoeker Nathan Russer constateerde dat Strava geanonimiseerde gegevens beschikbaar stelt, waarin te zien is waar gebruikers van de app het vaakst gaan sporten. Maar die gegevens laten dus ook activiteit zien in gevoelige gebieden zoals een CIA-basis op een verlaten vliegveld in Somalië en langs de grenzen van Noord-Korea. Strava laat naar aanleiding van de ontdekking weten gebruikers duidelijker in te zullen lichten over de privacyinstellingen. Eerder al verbood het Amerikaanse leger soldaten om de locatiegame Pokémon Go te installeren.

Op 27 juli 2020 wordt duidelijk dat fabrikant Garmin, bekend van gps-apparaten en sporthorloges, kampt met een grote storing.[4] De storing omvat onder andere de *Garmin Connect*-apps en -websites. Hierdoor kunnen gebruikers de clouddiensten van het bedrijf niet meer gebruiken en hun wearables ook niet meer lokaal synchroniseren met de bijbehorende apps. Later blijkt dat de storing veroorzaakt werd door een ransomware-aanval[5] waardoor de systemen op 23 juli versleuteld werden; vanaf 27 juli werden de getroffen systemen hersteld.[6] Garmin gaf daarbij aan geen indicatie te hebben dat klantgegevens verloren zouden zijn gegaan of zouden zijn gestolen. Desalniettemin waren sommige functies enkele dagen onbruikbaar, wat vervelend kan zijn voor gebruikers.

Over het algemeen kunnen verschillende soorten risico's onderscheiden worden als het gaat om eHealth-technologie[7] waaronder ook fysiologische wearables (Burg-

---

[3] www.nu.nl/internet/5107985/data-van-fitness-app-strava-toont-geheime-militaire-locaties.html

[4] https://tweakers.net/nieuws/170118/garmin-kampt-met-grote-storing.html

[5] Ransomware is een chantagemiddel op internet waarbij een computersysteem en/of de gegevens die erop staan door ransomware worden geblokkeerd. Vervolgens wordt van de gebruiker geld vraagt om de computer te ontgrendelen zodat het systeem of de gegevens weer toegankelijk worden.

[6] https://newsroom.garmin.com/newsroom/press-release-details/2020/Garmin-issues-statement-on-recent-outage/default.aspx

[7] eHealth is het toepassen van ICT ten dienste van de gezondheidszorg.

houts, 2015; Ossebaard et al., 2012). Hierbij gaat het om organisatiegebonden risico's, persoonsgebonden risico's en technologiegebonden risico's. Organisatiegebonden risico's hebben betrekking op bijvoorbeeld beperkte ondersteuning vanuit een organisatie voor de introductie van de technologie of werkprocessen en protocollen die niet goed zijn aangepast op de praktijk. Persoonsgebonden risico's hebben betrekking op bijvoorbeeld de mogelijkheid dat de technologie niet voldoende aansluit op de capaciteiten, wensen en de behoefte van de gebruiker waardoor de gebruiker de motivatie verliest om de toepassing te gebruiken. Organisatie- en persoonsgebonden risico's zijn belangrijk om in ogenschouw te nemen bij de introductie van nieuwe technologie, maar in dit rapport richten we ons alleen op technologiegebonden risico's.

Technologiegebonden risico's verwijzen naar zwakheden van de technologie zelf. Dit heeft bijvoorbeeld betrekking op een instabiel internetnetwerk, kwetsbare apparatuur, maar ook op de manier waarop verzamelde gegevens opgeslagen, beheerd en verspreid worden. Cornet en collega's (2017) beschrijven dat er bij ontwikkelaars van technologische zelfmeetapparatuur vaak nog te weinig aandacht is voor de veiligheid van producten. *First-to-market* zijn met een product is heel veel waard, ook als dat ten koste gaat van de veiligheid (Verbruggen & Wolters, 2017). Toch is voor het gebruik van fysiologische wearables in de justitiële context de keuze vooralsnog beperkt tot commerciële producten. Dit brengt risico's met betrekking tot de veiligheid met zich mee, maar ook onzekerheid of een aangeschafte wearable een jaar later nog wel leverbaar is en/of ondersteund wordt (en bijvoorbeeld nog beveiligingsupdates blijft krijgen). De razendsnelle ontwikkelingen leiden ertoe dat niet elke fabrikant het hoofd boven water kan houden.[8] Een mogelijk risico is dat bij een eventuele overname van een bedrijf de verzamelde (persoons)gegevens mee gekocht worden.[9] Zaken als veiligheid van de gegevens en privacy van de gebruiker (of de drager, zie ook box 1) spelen een grote rol in de mogelijke toepasbaarheid van fysiologische wearables in de justitiële context.

Box 1 Gebruiker en drager van wearables

Wearables zijn veelal ontwikkeld voor consumenten die geïnteresseerd zijn in hun eigen lichaamstoestand (in dit verband wordt ook wel de term *Quantified Self*, QS, gebruikt). In dit geval zijn de gebruiker en de drager dezelfde persoon. In dit rapport wordt echter voornamelijk het gebruik van wearables voor onderzoeks-, behandel- of toezichtdoeleinden besproken. In dit geval zijn de gebruiker en de drager niet dezelfde persoon.
De *gebruiker* (bijvoorbeeld een onderzoeker, behandelaar of toezichthouder) is degene die de gegevens verzamelt, opslaat, verwerkt, analyseert en eventueel verwijdert. Veelal is de gebruiker ook degene die de wearable aanschaft, de overeenkomst met de fabrikant aangaat en zijn of haar persoonlijke gegevens verstrekt hiervoor. In sommige gevallen is de gebruiker niet een individuele persoon, maar een organisatie, zoals DJI of het WODC, die de behandeling, het toezicht of het onderzoek uitvoert of laat uitvoeren.
De *drager* (bijvoorbeeld een justitiabele die deelneemt aan wetenschappelijk onderzoek of aan een pilot van behandelaars of toezichthouders) is degene die de wearable draagt en van wie de fysiologische gegevens worden verzameld.

[8] Een voorbeeld is het bedrijf Jawbone dat na financiële problemen in 2016 plotseling stopte met het produceren van fitnessarmbanden en ook geen ondersteuning meer bood, zie www.fithacking.nl/jawbone-support-klantenservice.

[9] Recent zijn er bijvoorbeeld zorgen over wat de overname van het bedrijf Fitbit door Google betekent voor de privacy van de gebruikers (European Data Protection Board, 2020a).

Veiligheid van de gegevens heeft betrekking op de beveiliging rondom gegevensopslag en -transport. Veiligheidsrisico's zijn onder te verdelen in security- en safetyrisico's (Aoyama et al., 2013). Securityrisico's worden intentioneel veroorzaakt, bijvoorbeeld wanneer systemen gericht worden aangevallen of aangetast door kwaadwillende personen. Safetyrisico's ontstaan zonder expliciete intenties, bijvoorbeeld door menselijke fouten, ontwerpfouten of storingen. Voor beide typen risico's geldt dat ze veroorzaakt kunnen worden door de wearable zelf, maar ook door de achterliggende infrastructuur, zoals het communicatienetwerk of de servers van de fabrikant. Beide typen worden, waar van toepassing, in dit rapport besproken. Denk aan vragen zoals: In hoeverre biedt de fabrikant bescherming tegen verlies van gegevens of ongeoorloofde toegang, zoals hacken? Hoe worden de verzamelde gegevens opgeslagen en gebeurt dit binnen een beveiligde omgeving? Hetzelfde geldt voor het transport van de gegevens van de wearable naar bijvoorbeeld een computer, is deze verbinding veilig?

Met *privacy* wordt in dit rapport bedoeld dat de verzamelde (persoons)gegevens van de drager beschermd worden om onthullingen te voorkomen.[10] Bedreigingen rondom privacy hangen sterk samen met veiligheidsrisico's. Wanneer de beveiliging van de wearable niet op orde is, wordt de kans op privacyschendingen groter, bijvoorbeeld de kans dat kwaadwillende personen toegang krijgen tot persoonsgegevens. In dit kader worden ten aanzien van de polsband onder andere de volgende vragen gesteld: Welke gegevens worden over de drager verzameld? Worden gegevens met anderen gedeeld? Indien dit gebeurt, met wie? Zijn gebruikers zich hiervan bewust? En in hoeverre kunnen gebruikers hier invloed op uitoefenen? Waar en hoe lang worden de gegevens vervolgens opgeslagen?

Naast de genoemde veiligheids- en privacyaspecten zijn ook *de validiteit, accuratesse en betrouwbaarheid* van de gegevensverzameling belangrijk bij de keuze voor bepaalde wearables. Hoewel deze aspecten geen onderdeel zijn van de centrale onderzoeksvraag van dit rapport, komen ze wel aan de orde. Bijvoorbeeld bij de vergelijking van de Empatica E4 met andere wearables (hoofdstuk 4) en in de gebruikersenquête (hoofdstuk 5). De validiteit van de metingen met een bepaald instrument heeft betrekking op de mate waarin de metingen weergeven wat het instrument pretendeert te meten. Onder accuratesse wordt verstaan de nauwkeurigheid van de metingen. Met betrouwbaarheid wordt de mate waarin gegevens altijd op dezelfde manier worden gemeten en niet vertekend of gewijzigd worden bedoeld. De laatste jaren wordt er steeds meer onderzoek verricht naar de validiteit, accuratesse en betrouwbaarheid van metingen met de Empatica E4 en andere vergelijkbare wearables. Hierin worden de metingen van deze wearables doorgaans vergeleken met metingen van professionele en geijkte laboratoriumapparatuur; de zogenoemde gouden standaard. De resultaten van enkele van deze onderzoeken bespreken we in paragraaf 2.4.

1.3 Relevante wetgeving omtrent persoonsgegevens en wearables

Binnen de justitiële context kunnen fysiologische wearables voor verschillende doeleinden worden ingezet. Te denken valt aan wetenschappelijk (gedrags)onderzoek, maar mogelijk in de toekomst ook aan gebruik in het kader van behandeling en reclasseringstoezicht (Cornet et al., 2017; De Kogel, 2019). De belangrijkste, rele-

[10] Dit wordt ook wel informationele privacy genoemd. De hier gehanteerde definitie (bescherming van informatie) is beperkter dan de definitie van privacy in de brede zin (het recht op een persoonlijke levenssfeer).

vante wetgeving voor de omgang met gegevens voor de verschillende doeleinden wordt hieronder uiteengezet.

De belangrijkste regels voor de omgang met persoonsgegevens in Nederland en de EU zijn vastgelegd in de Algemene Verordening Gegevensbescherming (AVG). De verplichtingen van de AVG zijn rechtstreeks van toepassing in Nederland. Waar de AVG ruimte laat voor nationale keuzes, zijn deze voor Nederland ingevuld in de Uitvoeringswet AVG (UAVG). De AVG geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is.

De AVG gaat over het rechtmatig omgaan met persoonsgegevens. Hierin staat bijvoorbeeld dat persoonsgegevens alleen verzameld mogen worden met een gerechtvaardigd doel, dat de verwerking moet passen bij het doel waarvoor ze worden verwerkt, dat de gegevens op een passende manier moeten zijn beveiligd en dat inbreuken in verband met persoonsgegevens (datalekken) gemeld moeten worden. Het verwerken van bijzondere persoonsgegevens, waaronder gegevens die met fysiologische wearables verzameld kunnen worden, zoals gezondheidsgegevens[11] en biometrische gegevens,[12] is verboden tenzij er een beroep kan worden gedaan op een wettelijke uitzondering én op een van de grondslagen voor het verwerken van gewone persoonsgegevens. Een uitzonderingsgrond is bijvoorbeeld de uitdrukkelijke toestemming van de betrokkene voor de verwerking van zijn/haar gegevens (*informed consent*). Ook het verwerken van strafrechtelijke persoonsgegevens is aan strenge voorwaarden gebonden.

Bij wetenschappelijk onderzoek dat wordt uitgevoerd in het algemeen belang ontstaat er conform de AVG, zoals uitgewerkt in de UAVG, een uitzondering op het verbod om bijzondere persoonsgegevens te verwerken en is er een grondslag voor deze verwerking (dit is dan wel toegestaan). Het is dan volgens de AVG strikt genomen niet per se nodig om schriftelijke toestemming van de betrokkene (bijvoorbeeld de drager van de wearable) te verkrijgen (als het vragen van uitdrukkelijke toestemming onmogelijk blijkt of een onevenredige inspanning kost).[13] Desalniettemin blijft de onderzoeker verantwoordelijk voor een goede bescherming van de persoonsgegevens en is het vanuit ethisch oogpunt aan te raden toch toestemming te vragen. Dit is bij uitstek het geval bij kwetsbare doelgroepen zoals gedetineerden. Het is daarom gebruikelijk bij DJI en andere justitiële organisaties dat altijd om toestemming wordt gevraagd, ook als er (ook) een andere rechtsgrond wordt gebruikt om de (bijzondere) persoonsgegevens te verwerken. In het geval van toestemming ontstaat er, ook als het niet om wetenschappelijke onderzoek gaat, een grondslag voor de verwerking van bijzondere persoonsgegevens. Een belangrijke voorwaarde is dan wel dat de toestemming in vrijheid gegeven is. Iemand moet de keuze hebben om te weigeren, zonder dat hier negatieve conse-

[11] Gezondheidsgegevens zijn persoonsgegevens over de fysieke of mentale gezondheid van een persoon. Voorbeelden zijn gewicht, hartslag, ziekterisico of verleende gezondheidsdiensten.

[12] Biometrische gegevens zijn persoonsgegevens die het resultaat zijn van een specifieke technische verwerking met fysieke, fysiologische of gedragsgerelateerde kenmerken van een persoon op grond waarvan eenduidige identificatie van die persoon mogelijk is of wordt bevestigd. Voorbeelden zijn vingerafdrukken, irispatronen, gezichtsprofielen, looppatronen, stemgeluiden en slaapritmes.

[13] Voor onderzoek dat onder de Wet medisch-wetenschappelijk onderzoek met mensen valt, geldt dat er altijd schriftelijke toestemming van de deelnemers nodig is.

quenties aan verbonden zijn. Met name wanneer er sprake is van een afhankelijkheidsrelatie tussen de betrokkene en de instantie die om de toestemming vraagt, is de vraag of toestemming vrij te geven is niet altijd eenvoudig te beantwoorden.

Bij het gebruik van wearables is in de toekomst ook de aankomende e-privacyverordening (ePV),[14] relevant. Deze verordening geeft een specificatie van en aanvulling op de algemene regels in de AVG, specifiek als het gaat om elektronische communicatiegegevens die als persoonsgegevens worden aangemerkt. De ePV regelt onder andere de uitwisseling van gegevens tussen apparaten zoals wearables.

Bij het gebruik van wearables kan daarnaast sprake zijn van de inzet van zogenoemde clouddiensten om gegevens niet lokaal maar op een server van een cloudprovider op te slaan. Afhankelijk van de provider kunnen de gegevens buiten de EU worden gebracht. De AVG kent een regime voor dergelijke internationale doorgiften; dit is niet zomaar toegestaan. Bij internationale doorgifte van persoonsgegevens kunnen daarnaast meerdere rechtsregimes van toepassing zijn en kunnen bijvoorbeeld ook aspecten van internationaal privaatrecht spelen.

Naast de AVG (en de UAVG) zijn er ten aanzien van de verwerking van persoonsgegevens in sommige domeinen (waaronder justitie en zorg) andere wetten van toepassing die wettelijke verplichtingen en wettelijke taken omschrijven op grond waarvan gegevens verwerkt mogen worden. Een aantal relevante wetten bespreken we hieronder. Welke wet of wetten precies van toepassing zijn op de verwerking van persoonsgegevens, is dus afhankelijk van het met de wearable beoogde gebruik. Voor wetenschappelijk onderzoek gelden deels andere wetten dan voor de tenuitvoerlegging van straffen of voor medische behandelingen.

Binnen de justitiële context is voor bepaalde taken van politie en justitie waarbij strafrechtelijke persoonsgegevens worden verwerkt niet de AVG van toepassing, maar geldt de Europese richtlijn gegevensbescherming opsporing en vervolging (Richtlijn (EU) 2016/680).[15] Deze richtlijn omvat – net als de AVG – regels voor de verwerking van persoonsgegevens en waarborgen rond de beveiliging en bescherming van persoonsgegevens. De richtlijn is van toepassing op de verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten, of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid (artikel 2, eerste lid, van de richtlijn). Bevoegde autoriteit is bijvoorbeeld DJI waaronder onder andere penitentiaire inrichtingen en tbs-klinieken vallen. Niet bevoegde autoriteiten in de zin van de richtlijn zijn bijvoorbeeld de Raad voor Strafrechtstoepassing en Jeugdbescherming (RSJ), Stichting Halt, en de reclasseringsinstellingen. Wanneer zij persoonsgegevens verwerken is de AVG daarop van toepassing. De verplichtingen in de richtlijn zijn omgezet in nationale wetgeving en werken niet rechtstreeks. In Nederland is de Europese richtlijn geïmplementeerd in de Wet justitiële en strafvorderlijke gegevens (Wjsg) en de Wet politiegegevens (Wpg). De Wjsg regelt het verwerken van justitiële gegevens (in persoonsdossiers) en de verwerking van strafvorderlijke gegevens. De Wjsg en de Wpg enerzijds en de AVG anderzijds sluiten elkaar qua toepassingsbereik uit.

---

[14] Voluit: Verordening van het Europees parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie. Deze verordening moet de bestaande e-privacyrichtlijn (Richtlijn 2002/58/EG) vervangen.

[15] Voor wat betreft het toepassingsbereik sluiten de AVG en de richtlijn elkaar wederzijds uit.

Wanneer het om justitiabelen gaat, zijn ook de beginselenwetten relevant. Dit zijn onder andere de Beginselenwet justitiële jeugdinrichtingen (Bjj), de Beginselenwet verpleging terbeschikkinggestelden (Bvt) en de Penitentiaire beginselenwet (Pbw). Hierin staan bepalingen over de verwerking van persoonsgegevens. Wanneer gegevens van justitiabelen worden verwerkt vanuit het oogpunt van zorg of behandeling (het dragen van de wearable wordt voorgeschreven door een arts), zijn daarnaast de Wet inzake de Geneeskundige Behandelovereenkomst (WGBO), de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz) (en het daaraan gerelateerde Besluit elektronische gegevensverwerking door zorgaanbieders) en de Wet forensische zorg (Wfz) relevant.

De WGBO regelt de behandelrelatie tussen hulpverlener (een individuele arts of instelling) en patiënt. In de WGBO staat onder andere dat de patiënt recht heeft op informatie in begrijpelijke taal over de gevolgen en risico's van de behandeling en over eventuele alternatieven. Voor iedere behandeling is toestemming van de patiënt vereist. In deze wet is daarnaast de inzage in en bewaartermijnen van medische dossiers geregeld. Een patiënt heeft recht op inzage in het dossier en niemand anders mag het dossier inzien, tenzij de patiënt daar toestemming voor geeft. Daarnaast kan de patiënt vragen om vernietiging van (een deel van) het medisch dossier. Nadere bepalingen over de omgang met het medische dossier, specifiek met betrekking tot de elektronische uitwisseling ervan, staan in de Wabvpz en het daaraan gerelateerde besluit. Het medisch beroepsgeheim is ook onderdeel van de WGBO: de zorgverlener moet vertrouwelijk met de patiëntgegevens omgaan. Gegevens uit het medisch dossier kunnen, conform de WGBO, onder bepaalde condities wel (zonder toestemming) verstrekt worden ten behoeve van wetenschappelijk onderzoek.[16]

De Wfz regelt de zorg aan justitiabelen die geestelijke gezondheidszorg, verslavingszorg of verstandelijke gehandicaptenzorg nodig hebben. Hierin zijn ook regels vastgelegd met betrekking tot gegevensuitwisseling tussen DJI, OM, reclassering en forensische zorgaanbieders. Conform de Wfz kunnen persoonsgegevens verstrekt worden voor wetenschappelijk onderzoek, mits de onderzoeker waarborgen heeft getroffen voor de bescherming van de persoonlijke levenssfeer van de betrokkenen.

Wanneer persoonsgegevens van justitiabelen met het oog op wetenschappelijk onderzoek worden verwerkt, is de AVG op die verwerkingen van toepassing. De verstrekking van de gegevens moet dan wel rechtmatig zijn conform de voor de betreffende gegevens geldende wet- en regelgeving (bijvoorbeeld de Wjsg, WGBO of Wfz). Zodra de gegevens aan een onderzoekende partij zijn verstrekt, is de AVG van toepassing. De verwerking moet dan rechtmatig zijn. In artikel 5 (beginselen inzake verwerking), artikel 89 (waarborgen wetenschappelijk onderzoek), artikel 9 (verwerking bijzondere persoonsgegevens) en artikel 10 (verwerking strafrechtelijke persoonsgegevens) van de AVG zijn de bepalingen daarover vastgelegd.

Indien wearables worden gebruikt voor medisch-wetenschappelijk onderzoek kan daarnaast de Wet medisch-wetenschappelijk onderzoek met mensen (WMO) van toepassing zijn.[17] In deze wet staat onder andere dat de proefpersonen schriftelijke

[16] De WGBO is van toepassing op medisch-wetenschappelijk onderzoek dat niet onder de reikwijdte van de Wet medisch-wetenschappelijk onderzoek met mensen (WMO) valt. Ook op medisch-wetenschappelijk onderzoek dat wel onder de reikwijdte van de WMO valt, kan de WGBO aanvullend van toepassing zijn.

[17] Zie www.ccmo.nl/onderzoekers/wet-en-regelgeving-voor-medisch-wetenschappelijk-onderzoek/uw-onderzoek-wmo-plichtig-of-niet voor een overzicht van onderzoek dat onder de WMO valt.

toestemming moeten geven voor deelname aan het onderzoek. De deelnemers moeten daarbij voorafgaand aan het geven van toestemming schriftelijk geïnformeerd worden over het doel, de aard en duur van het onderzoek en de risico's van deelname. De Centrale Commissie Mensgebonden Onderzoek (CCMO) waarborgt de bescherming van proefpersonen betrokken bij medisch-wetenschappelijk onderzoek, middels toetsing aan de daarvoor gestelde wettelijke bepalingen en met inachtneming van het belang van de voortgang van de medische wetenschap. Onderzoek dat onder de WMO valt, moet door een medisch-ethische toetsingscommissie (METC) worden goedgekeurd. Ook wanneer toetsing door een METC niet verplicht is, is het bij onderzoek met justitiabelen aan te bevelen om het onderzoeksprotocol te laten toetsen op de ethische aspecten door een ethische commissie (ETC). Eén van de redenen daarvoor is dat justitiabelen, wanneer een vrijheidsbeperkende straf of maatregel is opgelegd, mogelijk moeilijker in vrijheid kunnen beslissen over het al dan niet deelnemen aan het onderzoek. Een tweede reden is dat onder justitiabelen veel psychische en andere problematiek voorkomt waardoor zij een kwetsbare groep vormen.

Een wearable of app kan in een aantal gevallen als medisch hulpmiddel worden beschouwd (van Drongelen et al., 2019). In dat geval dient ook een toetsingsprocedure voor een medisch hulpmiddel te worden gevolgd. Hierop is nu nog de Wet op de medische hulpmiddelen, het Besluit medische hulpmiddelen en de Europese richtlijn medische hulpmiddelen (*Medical Devices Directive*, MDD) van toepassing. Vanaf mei 2021 geldt de Europese verordening Medische hulpmiddelen (*Medical Devices Regulation*, MDR). Vanaf dan geldt de nieuwe Nederlandse Wet medische hulpmiddelen en wordt het Besluit medische hulpmiddelen ingetrokken.

1.4 Privacy paradox

Hoewel gebruikers, zowel consumenten of zorgverleners, vaak wel weten dat er privacykwesties spelen bij technologische apparatuur, waaronder wearables, wordt er toch gretig gebruik van gemaakt. De markt voor wearables blijft razendsnel groeien.[18] Tegelijkertijd maken verschillende partijen zich zorgen over de privacy van de dragers van wearables, zoals recent ook bleek rondom de overname van Fitbit door Google (European Data Protection Board, 2020a). Recent voerde Het Financieele Dagblad (FD) een onderzoek uit naar slimme horloges en polsbandjes op de consumentenmarkt.[19] Hieruit bleek dat, volgens het FD, de fabrikanten hiervan niet aan alle regels van de AVG voldoen. Dit is problematisch, omdat dergelijke wearables steeds meer gezondheidsgegevens zijn gaan registreren en deze gegevens juist extra beschermd zouden moeten worden.

In de literatuur wordt bovengenoemd fenomeen ook wel de 'privacy paradox' genoemd. Deze paradox verwijst naar het verschil tussen de houding van gebruikers ten opzichte van privacy-kwesties en het daadwerkelijke gedrag (Kokolakis, 2017). Consumenten zeggen hun privacy belangrijk te vinden, maar doen tegelijkertijd weinig om hun privacy te beschermen en blijven onveilige producten gebruiken. Er zijn verschillende theorieën over waarom deze paradox bestaat en zo hardnekkig is (Barth & De Jong, 2017). Zo is de drang naar deelname aan online sociale netwerken vaak sterker dan geobserveerde risico's. De voordelen wegen dan op tegen de nadelen. Maar vaak zijn er ook geen, of geen goede alternatieven. Bij veel wear-

[18] www.counterpointresearch.com/global-smartwatch-market-revenue-h1-2020/

[19] https://fd.nl/futures/1355712/fabrikanten-slimme-horloges-voldoen-niet-aan-europese-privacynorm

ables maakt bijvoorbeeld 'het delen van gebruikersgegevens door de fabrikant met derden' deel uit van de gebruiksvoorwaarden van de fabrikant die geaccepteerd moeten worden om het product te kunnen gebruiken. Ook ontbreekt vaak de kennis om de instellingen van de wearable op die manier aan te passen dat je als gebruiker (enigszins) beschermd blijft. Het FD constateerde dat de privacyverklaring (die de gebruiker houvast zou moeten bieden over wat er met de gegevens gebeurt), vaak onbegrijpelijk en erg juridisch is. Het is dus de vraag of er wel voldoende informatie aanwezig is voor de gebruiker om hierin een goede afweging te kunnen maken.

1.5 Onderzoeksvragen

Dit casusonderzoek geeft een beknopt beeld van de dataveiligheid en privacy bij één fysiologische wearable, vergelijkt de belangrijkste risico's met de risico's bij andere wearables, en schetst de ervaringen van een klein aantal gebruikers in een professionele (justitiële) context.

De volgende deelvragen staan centraal in dit onderzoek:

1 Wat gebeurt er met de fysiologische gegevens van de Empatica E4 nadat deze verzameld zijn door de gebruiker met betrekking tot: gegevensopslag, gegevenstransport en toegang tot de gegevens door derden?
2 Wat zijn de risico's daarbij voor de veiligheid van de gegevens en voor de privacy van de drager? En hoe zien de risico's en de geboden functionaliteit eruit in vergelijking met andere wearables?
3 Welke kennis, ervaringen en zorgen hebben professionele gebruikers van de Empatica E4 met betrekking tot gegevensopslag, toegang tot gegevens door derden en privacy?
4 Wat betekenen de antwoorden op de deelvragen voor het gebruik van de Empatica E4 en andere fysiologische wearables in de justitiële context?

1.6 Methoden

Deelvragen 1 en 2 zijn beantwoord door deskresearch uit te voeren. Er is gezocht naar informatie op de website van Empatica over de veiligheid en privacy van (de gegevens verzameld met) de Empatica E4. De privacyverklaring van Empatica is bekeken, er is een account bij Empatica aangemaakt en de Empatica E4 is in de praktijk uitgeprobeerd. Vervolgens zijn een aantal aanvullende vragen aan Empatica gesteld over de privacyverklaring en een aantal punten met betrekking tot de opslag en het gebruik van de fysiologische gegevens door de fabrikant (zie bijlage 3). Ook is de Privacy Officer van het WODC bevraagd.

Voor de vergelijking van de dataveiligheid en privacy van de Empatica E4 met die van andere wearables (onderdeel van deelvraag 2) is als volgt te werk gegaan: we hebben eerst naar relevante wearables gezocht door verschillende zoekopdrachten op internet uit te voeren[20], door het vraag & antwoord forum van Research Gate te raadplegen waarin onderzoekers ervaringen met betrekking tot wearables uitwisse-

[20] Hierbij hebben we in de Google-zoekmachine de volgende zoektermen gebruikt: 'alternatives to Empatica E4', 'wearable EDA sensor', 'wearable GSR sensor', 'wearable EDR sensor', 'wearable PPG sensor', 'wearable ECG sensor', 'wearable EDA monitor', 'wearable GSR monitor', 'wearable EDR monitor', 'wearable PPG monitor', 'wearable ECG monitor', 'wearable for research on stress' en 'wearable for research on emotion'.

len,[21] en door experts te bevragen op het Wearable in Practice Symposium gehouden op 3 oktober 2019. Vervolgens is gekeken welke sensoren de gevonden wearables bevatten. Voor onze analyse hebben we alleen de wearables geselecteerd die ruwweg dezelfde sensoren bevatten als de Empatica E4 of die minimaal huidgeleiding kunnen meten.[22] Concreet betekent dit dat we alleen naar wearables hebben gekeken die minstens huidgeleiding en/of hartslag kunnen meten en daarnaast idealiter ook beweging en/of huidtemperatuur. Voor de geselecteerde wearables is op de website van de fabrikant gezocht naar handleidingen die duidelijk maken hoe de wearable gebruikt kan/moet worden en naar eventuele privacyverklaringen.

Deelvraag 3 is beantwoord door middel van een korte enquête (bijlage 2). Deze enquête is uitgezet bij alle bezoekers van de bijeenkomst van het netwerk Wearables in Practice op 6 april 2018 met ervaring als professionele gebruiker van de Empatica E4. In de enquête werd gevraagd naar de kennis, ervaring en zorgen van de gebruikers met betrekking tot het transport, de opslag en het beheer van de gegevens. Wat gebeurt er met de verzamelde gegevens, en wie heeft daar toegang toe? En in hoeverre zijn de (professionele) gebruikers zich hier bewust van? In totaal hebben tien respondenten de enquête (geheel of gedeeltelijk) ingevuld. Met twee gebruikers uit de justitiële context is nader overleg gepleegd over het gebruik van de Empatica E4.

Deelvraag 4 is beantwoord op basis van onze bevindingen met betrekking tot de eerste drie vragen.

1.7 Beperkingen van dit casusonderzoek

Het hoofddoel van dit casusonderzoek is om het bewustzijn over dataveiligheid en privacyaspecten bij het gebruik van fysiologische wearables in de justitiële context te vergroten. De aanpak die we hebben gekozen is om deze aspecten te illustreren aan de hand van één specifiek instrument; de Empatica E4. In dit onderzoek is de Empatica E4 vergeleken met een aantal andere wearables. Hierbij hebben we enerzijds gekeken naar de geboden functionaliteit en anderzijds naar de dataveiligheid en privacy. Deze vergelijking is echter niet uitputtend. Wij hebben niet voor meerdere wearables alle risico's met betrekking tot dataveiligheid en privacy volledig in kaart kunnen brengen omdat wij de gegevens daarover hebben verzameld via openbare bronnen als websites. Deze bronnen omvatten wat dit betreft niet altijd alle details. Aan de andere kant denken we dat we met het gedetailleerd bestuderen van dit ene instrument het doel van bewustwording voldoende kunnen bereiken, juist ook omdat dit aanvankelijk gekozen is als meest geschikt voor gebruik in de justitiële context. Een beperking is verder dat de gebruikerservaringen onderzocht zijn in een zeer kleine steekproef (n=10). Dit komt doordat het aantal gebruikers van de Empatica E4 in Nederland beperkt is. Deze steekproef omvat nagenoeg alle ons bekende gebruikers in Nederland. Daarnaast heeft deze gebruikersraadpleging al geruime tijd geleden plaatsgevonden, nog voordat de AVG in werking trad, en kan de kennis van de gebruikers inmiddels toegenomen zijn.

---

[21] Hierbij hebben we op het forum de zoekterm 'Empatica E4' gebruikt. Hierbij vonden we de volgende relevante vragen: www.researchgate.net/post/Empatica_E4_any_good_for_research? en www.researchgate.net/post/Can_anyone_recomend_good_stress_monitoring_device_during_normal_activity_enable_to_measure_for_long_time_24h?

[22] Een aantal van de gevonden/gesuggereerde wearables was op het moment van onderzoek niet meer (bijvoorbeeld de Microsoft Band 2) of nog niet beschikbaar, deze zijn daarom niet nader bekeken.

1.8 Leeswijzer

In hoofdstuk 2 zal de werking van de in dit rapport onderzochte fysiologische wearable, de Empatica E4, beschreven worden. Vervolgens zal in hoofdstuk 3 voor dit product de opslag van de verzamelde fysiologische gegevens, het transport van de gegevens en de toegang tot de gegevens onderzocht worden, en besproken worden wat dit betekent voor de veiligheid van de gegevens en de privacy van de drager. In hoofdstuk 4 wordt deze wearable vergeleken met andere beschikbare wearables. Hierbij wordt enerzijds gelet op de beschikbare functionaliteit en anderzijds op de dataveiligheid en privacy. Vervolgens worden in hoofdstuk 5 de resultaten van een korte enquête besproken die is gehouden onder een klein aantal professionals die de Empatica E4 in hun werk hebben gebruikt. In de discussie (hoofdstuk 6) wordt tot slot ingegaan op de vraag wat de bevindingen naar aanleiding van de onderzoeksvragen betekenen voor het gebruik van fysiologische wearables zoals de Empatica E4 in de justitiële context.

2 De Empatica E4

2.1 Inleiding

Figuur 1 De Empatica E4

Bron: verkregen van E4-presskit

De Empatica E4 (zie figuur 1) is een polsband ontwikkeld door prof. Rosalind Picard van het Massachusetts Institute of Technology (MIT). Deze polsband meet door middel van vier sensoren verschillende fysiologische signalen. De polsband is uitdrukkelijk bedoeld voor gebruik door onderzoekers in klinische studies. Daarnaast kan de Empatica E4 gebruikt worden door medische professionals om van een afstand de gezondheid van patiënten te monitoren.[23] Empatica verkoopt de polsband uitsluitend aan gebruikers verbonden aan onderzoeksinstellingen (zoals ziekenhuizen, farmaceutische bedrijven of universiteiten)[24] en raadt persoonlijk gebruik af.[25] De Empatica E4 is daar ook minder geschikt voor doordat deze, afgezien van de relatief hogere prijs, niet zoals typische wearables een eenvoudige userinterface biedt (bijvoorbeeld een scherm waarop de metingen zijn af te lezen) en alleen toegang biedt tot ruwe gegevens die lastig te interpreteren zijn zonder technische expertise. Voor persoonlijk gebruik heeft Empatica een ander product op de markt gebracht: de *Embrace* en de gereviseerde versie *Embrace2*. Ook deze polsband kan overigens ingezet worden voor onderzoeksdoeleinden. De *Embrace2* en het gebruik ervan voor onderzoek bespreken we in paragraaf 4.2.

Doordat de Empatica E4 voornamelijk voor onderzoeksdoeleinden wordt gebruikt, is er hier sprake van een afzonderlijke drager (de onderzoeksdeelnemer van wie de fysiologische gegevens verzameld worden) en gebruiker (een onderzoeker die fysiologische gegevens van de drager verzamelt en analyseert, zie ook box 1). Het is de gebruiker die een account voor de Empatica E4 aanmaakt en een overeenkomst

[23] www.empatica.com/en-eu/care/

[24] www.empatica.com/connect/privacy

[25] https://support.empatica.com/hc/en-us/articles/203934675-Is-the-E4-suitable-for-personal-use-

aangaat met Empatica. Over deze persoon verzamelt Empatica gegevens die nodig zijn voor het uitvoeren van de overeenkomst en de bedrijfsactiviteiten. Bij de aanschaf van de polsband deelt de gebruiker bijvoorbeeld zijn/haar naam, contactgegevens zoals telefoonnummer en e-mailadres, een verzendadres en betaalgegevens. De belangrijkste en grootste hoeveelheid gegevens die door Empatica wordt opgeslagen bestaat echter uit de metingen van de sensoren. Deze betreffen de drager van de polsband. De analyse in hoofdstuk 3 betreft alleen deze fysiologische gegevens van de drager.

Hieronder bespreken we eerst de specificaties van de polsband en de sensoren die deze bevat (paragraaf 2.2). Vervolgens lichten we in paragraaf 2.3 het gebruik van de polsband en het benodigde account toe. In paragraaf 2.4 beschrijven we het onderzoek dat is gedaan naar de validiteit, accuratesse en betrouwbaarheid van de Empatica E4.

2.2 Specificaties

De band meet vier verschillende fysiologische signalen: 1) huidgeleiding, 2) pols/hartslag, 3) beweging en 4) (huid)temperatuur (zie ook figuur 2). Huidgeleiding, ook wel bekend als elektrodermale activiteit (EDA), galvanische huidreactie (GSR) of elektrodermale respons (EDR), is de meting van elektrische geleiding of weerstand van de huid. Dit wordt doorgaans gedaan op de handpalmen, vingers of voetzolen. Er worden twee elektroden geplaatst die een kleine continue stroom door het lichaam en langs het huidoppervlak sturen. Wanneer zweetklieren geactiveerd worden, neemt de geleiding van de huid toe (hoe meer zweet, hoe meer geleiding). Hiermee kan inzicht worden verkregen in veranderingen in activatie van het sympathisch (SNS) zenuwstelsel (sympathische activiteit activeert namelijk de zweetproductie), waarmee een inschatting gemaakt kan worden van de hoeveelheid stress of opwinding. De Empatica E4 bevat een EDA-sensor die bestaat uit twee elektrodes aan de onderkant van de pols. Voor het meten van de hartslag bevat de Empatica E4 een fotoplethysmograaf (PPG). Deze sensor bepaalt met verschillende kleuren licht (LEDs) wanneer er bloed door de aderen stroomt. Dit heet de *Blood Volume Pulse* (BVP). Hieruit kunnen de hartslag (*Heart Rate*, HR), de tijd tussen elke hartslag de (*inter-beat-interval*, IBI) en de variatie daarin (*Heart Rate Variability*, HRV) afgeleid worden. Een andere manier om de hartactiviteit te meten is met elektroden die op een borstband worden geplaatst (een zogenoemde ecg-sensor). Een ecg registreert de elektrische prikkels die de spiercellen in het hart laten samentrekken direct. Deze manier van meten is preciezer dan metingen met een PPG-sensor. Beweging wordt door de Empatica E4 gemeten met een accelerometer op drie dimensies: boven/onder, links/rechts, voor/achter. Tot slot wordt de huidtemperatuur (en in sommige gevallen ook de omgevingstemperatuur) gemeten met een infrarood thermodetector. De technische specificaties van de vier sensoren zijn weergegeven in box 2.

Box 2 Technische specificaties van de vier sensoren van de Empatica E4

1 Huidgeleiding: EDA-sensor. Sampling-frequentie: 4 Hz, resolutie: 1 digit ~ 900 pSiemens, bereik: 0,01 µSiemens - 100 µSiemens.
2 Hartslag: Fotoplethysmograaf. Sampling-frequentie: 64 Hz, resolutie: 0.9 nW / digit.
3 Beweging: 3-Axiale accelerometer. Sampling-frequentie: 32 Hz, resolutie: 8 bits van het gekozen bereik, bereik: ±2g (±4g of ±8g met custom firmware).
4 Temperatuur: Infrarood thermodetector. Sampling-frequentie: 4 Hz, resolutie: 0,02°C, bereik: -40 - 85°C (omgevingstemperatuur) of -40 - 115°C (huidtemperatuur).

Figuur 2 De vier sensoren van de Empatica E4

Bron: verkregen van www.empatica.com

2.3 Gebruik van het apparaat

De Empatica E4-polsband kan op twee manier gebruikt worden (zie ook figuur 3): in combinatie met een app op een mobiel apparaat (dit is de streamingmodus, in figuur 3 gemarkeerd met een 2) of door verbinding te maken met een computer (dit is de opnamemodus, gemarkeerd met een 1).

Figuur 3 Verschillende manier om de Empatica E4 te gebruiken

Bron: aangepast van https://e4.empatica.com

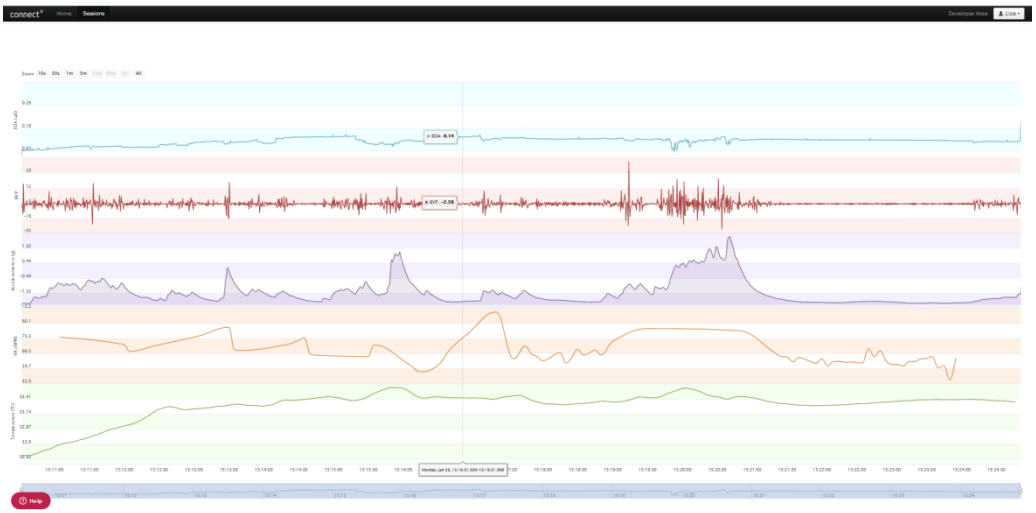
Met de app op het mobiele apparaat kan de gebruiker live de metingen van de sensoren zien. Zonder gebruik van de app krijgt de gebruiker geen realtime informatie. De band zelf heeft namelijk geen scherm of display om waardes op te tonen en op de computer kan de gebruiker de metingen alleen achteraf inzien en niet in real time. Om de Empatica E4 te kunnen gebruiken is er een *E4 Connect*-account nodig. Wat dit account inhoudt wordt hieronder in paragraaf 2.3.3 uitgebreider beschreven. Door in te loggen op de bijbehorende *E4 Connect*-website (gemarkeerd met een 3 in figuur 3) kunnen de metingen achteraf bekeken en beheerd worden.

Een dergelijke omgeving waarin gegevens niet lokaal bij de gebruiker, maar op de servers van een derde partij worden opgeslagen, wordt ook wel een cloud of cloudomgeving genoemd. De gegevens in de cloud zijn vanaf ieder apparaat met een internetverbinding toegankelijk. Empatica biedt met *E4 Connect* niet alleen gegevensopslag, maar ook een website aan (ook wel een dashboard genoemd), waarmee de gegevens bekeken en beheerd kunnen worden.

Wanneer de band in combinatie met de app op een mobiel apparaat (een smartphone of tablet) gebruikt wordt, worden de verzamelde gegevens na afloop van de meting direct en automatisch opgeslagen in het *E4 Connect*-account van de gebruiker. Via de *E4 Connect*-website[26] kunnen de opgeslagen gegevens achteraf geraadpleegd worden (zie een voorbeeld in figuur 4). Als de band niet gebruikt wordt met de app, dienen de gegevens handmatig uitgelezen te worden. Dit kan door de band met een USB-kabel aan een computer (een pc of laptop) te koppelen en vervolgens de gegevens van de polsband te halen, op de computer op te slaan en naar het *E4 Connect*-account te sturen. Daarna zijn deze gegevens online via de genoemde website te raadplegen. Beide manieren van gebruik worden hieronder nader toegelicht.

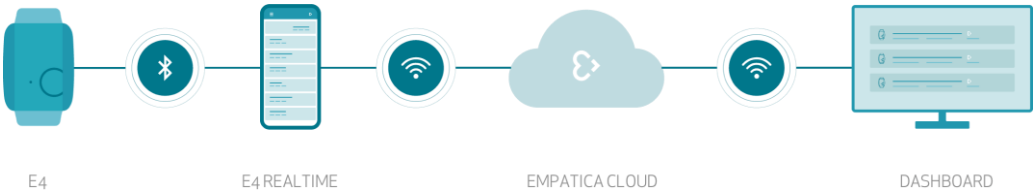
[26] www.empatica.com/connect/sessions.php

Figuur 4 Fysiologische gegevens verzameld door een van de auteurs op 29 januari 2018



2.3.1 Streamingmodus

Figuur 5 Gebruik van de Empatica in streamingmodus



Bron: verkregen van www.empatica.com/assets/images/e4/2/streaming_system-lg-xhdpi.png

Voor de streamingmodus (zie figuur 5) is een speciale app voor het mobiele apparaat (een smartphone of tablet draaiende op *iOS* of *Android*) nodig genaamd *Empatica E4 Realtime* (zie figuur 6). De band maakt dan via bluetooth draadloos verbinding met het mobiele apparaat waarop de app geïnstalleerd is. In de app kunnen de metingen live gevolgd worden. Deze gegevens worden vervolgens automatisch geüpload naar het *E4 Connect*-account van de gebruiker zodra de sessie is beëindigd. Dit gebeurt via de internetverbinding van het mobiele apparaat. De Empatica E4 heeft zelf geen directe verbinding met het internet. Na afloop van de sessie kunnen de metingen ook nog via de *E4 Connect*-website bekeken worden.

Figuur 6 De E4 Realtime app

Bron: verkregen van E4-presskit

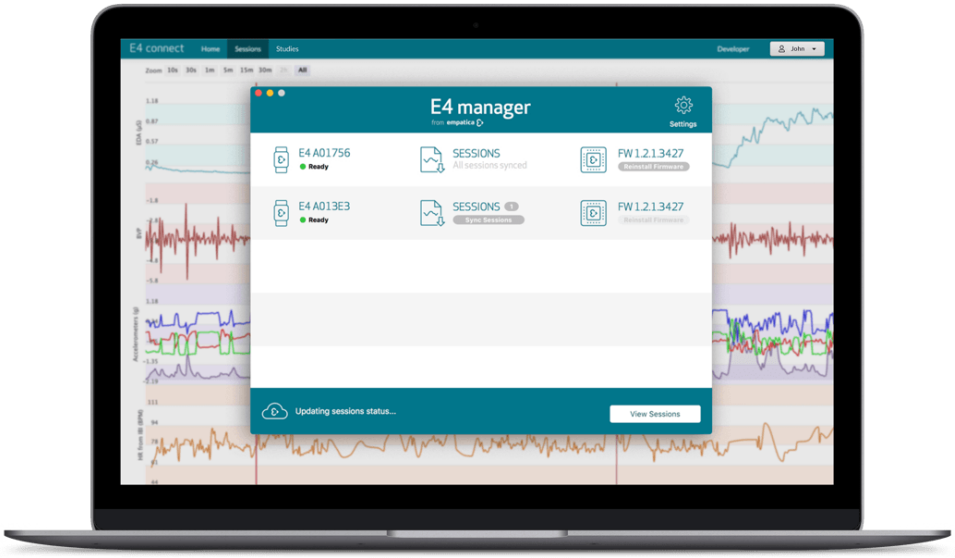
2.3.2 Opnamemodus

Figuur 7 Gebruik van de Empatica in opnamemodus

Bron: verkregen van www.empatica.com/assets/images/e4/2/recording_system-lg-xhdpi.png

In de opnamemodus (zie figuur 7) worden de metingen eerst in het interne geheugen (*flash memory*) van de polsband opgeslagen (maximaal 36 uur, synchronisatie elke vijf seconden). De gegevens kunnen handmatig uitgelezen worden door verbinding te maken met een computer via USB. Hiervoor moet een speciaal programma genaamd *E4 Manager* (zie figuur 8) gebruikt worden. Hiermee worden de gegevens via de internetverbinding van de betreffende computer naar het *E4 Connect*-account van de gebruiker gestuurd. Het computerprogramma *E4 Manager* biedt geen mogelijkheden om de gegevens visueel in te zien; het zorgt er alleen voor dat de gegevens van de polsband worden gedownload en naar *E4 Connect* worden geüpload. Voor het bekijken van de gegevens is de *E4 Connect*-website beschikbaar die via een webbrowser te benaderen is.

Figuur 8 Het E4 Manager programma



Bron: verkregen van www.empatica.com/assets/images/e4/2/e4manager-lg-xhdpi.png

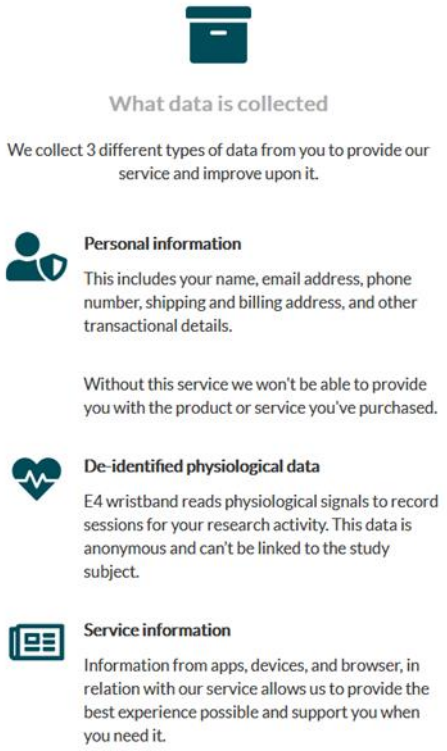
2.3.3 Het E4 Connect-account en de privacyverklaring

Het registreren van een *E4 Connect*-account is vereist voordat gebruik kan worden gemaakt van de diensten van Empatica, waaronder de *E4 Connect*-website, *E4 Manager* en de *E4 Realtime-app*. Bij het aanmaken van een account dient de gebruiker verschillende (persoons)gegevens aan Empatica te verstrekken: e-mailadres, voornaam en achternaam, en de naam van het bedrijf, de universiteit of het ziekenhuis waaraan hij/zij verbonden is. Deze gegevens heeft Empatica enerzijds nodig voor het uitvoeren van de overeenkomst met de gebruiker zoals het innen van betalingen, het leveren van services, (technische) ondersteuning en het afhandelen van klachten. Anderzijds hebben zij de gegevens nodig voor het uitvoeren van hun bedrijfsactiviteiten (een gerechtvaardigd belang in AVG-termen), bijvoorbeeld voor het uitvoeren van tests en updates van de polsband en meer in het algemeen het optimaliseren van hun diensten aan de gebruikers. Daarnaast worden deze gegevens gebruikt voor marketingdoeleinden.

Bij het aanmaken van het *E4 Connect*-account moet de gebruiker de privacyverklaring[27] lezen en aanvaarden. Hierbij wordt stap-voor-stap uitgelegd welke gegevens er door Empatica verzameld worden (zie figuur 9). Naast de persoonsgegevens van de gebruiker en de fysiologische gegevens van de drager, verzamelt Empatica ook (technische) service-informatie vanuit applicaties, apparaten en webbrowsers.

[27] www.empatica.com/connect/privacy.php. Aanvullende informatie is te vinden op: https://support.empatica.com/hc/en-us/articles/202524239-What-does-Empatica-do-to-protect-end-user-privacy en https://support.empatica.com/hc/en-us/articles/360000878346-GDPR-FAQs-for-Researchers-with-E4.

Figuur 9 Toelichting over de gegevensverzameling door Empatica bij het aanmaken van een E4 Connect-account



De persoonsgegevens van de gebruiker worden door Empatica gebruikt voor contractuele, bedrijfsvoerings- en marketingdoeleinden. De gegevens kunnen daarom gedeeld worden met derden. De verzamelde persoonsgegevens kunnen volgens de privacyverklaring overgedragen worden naar landen binnen en buiten de EU, voornamelijk naar de Verenigde Staten.

Conform de AVG heeft iedereen met een *E4 Connect*-account het recht om op te vragen welke persoonsgegevens er bij Empatica zijn opgeslagen. Dit kan door een e-mail naar Empatica te sturen. Iedereen heeft daarnaast het recht om het account te laten verwijderen, persoonsgegevens te laten verwijderen of te laten anonimiseren. Daarnaast kan iedere gebruiker bezwaar maken tegen het verwerken van de gegevens of verzoeken de verwerking te beperken. De gebruiker kan daarnaast een elektronische kopie van de persoonsgegevens opvragen.

Empatica verzamelt behalve de fysiologische gegevens geen persoonsgegevens van de dragers van de Empatica E4, raadt persoonlijk gebruik af (de polsband is bedoeld voor onderzoeksdoeleinden) en vraagt gebruikers (de onderzoekers) om geen persoonlijke informatie over de dragers met hen te delen. Conform de privacyverklaring van de Empatica E4, die de gebruiker moet aanvaarden bij het aanmaken van een *E4 Connect*-account, gaat de gebruiker ermee akkoord dat '*Empatica does not have access to the final users wearing the Device'* en '*that only the user has access to the personal information of the people physically wearing the Device*.' De fysiologische gegevens (van de drager van de polsband) zijn als gevolg hiervan niet direct herleidbaar tot individuele personen (ze zijn alleen gekoppeld aan het account van de gebruiker). Empatica stelt dat de verzamelde fysiologische gegevens daarmee

'effectief anoniem' zijn en beschouwt ze niet als persoonsgegevens. '*The data housed in E4 connect cannot be matched with the individuals physically wearing the device. Empatica will not access personal data from final users (study participants). Accounts are associated with the researcher, not final users, so data is effectively anonymous.*'[28] De privacyverklaring heeft daarom geen betrekking op deze gegevens en gaat heel specifiek (en alleen) over de persoonsgegevens van de gebruiker. In paragraaf 3.5 beschrijven we wat dit betekent voor de privacy van de gegevens en wat nodig is om de privacy van de dragers te waarborgen.

2.3.4 Apps van derden

Het is niet strikt noodzakelijk om *E4 Connect* en de app van Empatica te gebruiken om de Empatica E4 te kunnen uitlezen. Ontwikkelaars kunnen namelijk een ontwikkelaccount aanvragen om een eigen app voor *iOS* of *Android* te bouwen. Dit vergt wel de nodige deskundigheid en ervaring met het ontwikkelen van apps. Ontwikkelaars kunnen hiervoor de *software development kit* (SDK)[29] van Empatica gebruiken. Door een eigen app te ontwikkelen kan voorkomen worden dat de gegevens in de cloudomgeving van Empatica terecht komen.

Er zijn daarnaast verschillende Nederlandse partijen die apps hebben ontwikkeld of aan het ontwikkelen zijn die werken met de Empatica E4 of zouden kunnen werken met de Empatica E4. Deze apps staan helemaal los van de cloudomgeving van Empatica en maken gebruik van hun eigen cloudomgeving of dashboard. Een voorbeeld is de *HUME*-app van Mentech Innovation.[30] Dit is een cloud-gebaseerd streamingplatform, dat wearables zoals de Empatica E4 uitleest, en op basis van de gegevens spanning en spanningsopbouw laat zien. Daarnaast is er de *GRIP*-app (wat staat voor Goede Reactie Is Preventie) ontwikkeld door De Waag.[31] Deze app gebruikt momenteel een Polar borstband met een hartslagsensor, maar zou aangepast kunnen worden om ook de Empatica E4 te gebruiken. De *GRIP*-App is erop gericht om oplopende spanning of boosheid te signaleren.

2.4 Validiteit, accuratesse en betrouwbaarheid

Enkele kleinschalige onderzoeken (maximaal 20 deelnemers) laten als voorlopig resultaat zien dat de Empatica E4 voldoende betrouwbaar en accuraat de hartslag en de hartslagvariabiliteit meet in rust, maar dat bij handbewegingen de kwaliteit van de metingen sterk achteruit gaat (Pietilä et al., 2017, McCarthy et al. 2016; Lam et al., 2018, Ollander et al., 2016). Ook een recenter onderzoek, waarin de Empatica E4 is vergeleken met de VU-AMS als gouden standaard, laat zien dat de Empatica E4 accurate metingen van hartslag en hartslagvariabiliteit levert in rust (Schuurmans et al, 2020). Een ander recent onderzoek waarin meerdere wearables zijn vergeleken met als gouden standaard de Holter ecg laat ook zien dat de Empatica E4 goed werkt in rust, maar minder geschikt is voor ambulant gebruik of tijdens activiteiten met hoge intensiteit in termen van beweging of emoties (Barrios et al.,

[28] https://support.empatica.com/hc/en-us/articles/202524239-What-does-Empatica-do-to-protect-end-user-privacy-

[29] Een SDK biedt hulpmiddelen voor het ontwikkelen van software voor een bepaald type hardware (in dit geval de Empatica E4) en/of besturingssysteem (in dit geval *iOS* of *Android*).

[30] https://mentechinnovation.eu/product

[31] https://kfz.nl/projecten/call-2014-30-3 en www.wearemoose.com/cases/grip-app-de-waag

2019). Een groter onderzoek onder 40 gezonde deelnemers laat zien dat de accuratesse van de hartslagmeting in alle condities goed is, maar dat de accuratesse van de hartslagvariabiliteitsmeting voldoende is in rust maar slechter wordt bij (hand-) bewegingen en ook bij cognitieve en emotionele stress (Meghini et al., 2019).

Daarnaast is er verkennend onderzoek gedaan naar de accuratesse van de huidgeleidingssensor van de Empatica E4. Deze is lastig vast te stellen doordat huidgeleiding gemeten op de pols (zoals met de Empatica E4) onvergelijkbaar is met huidgeleiding gemeten op de vingers (zoals in een laboratoriumsetting gebruikelijk is). Deze eerste onderzoeken laten zien dat de huidgeleidingsmeting van de Empatica E4 relatief gevoelig is voor het meten van emotionele stress, zo laten de meeste proefpersonen bijvoorbeeld een stijging van de huidgeleiding zien tijdens een '*public speaking task*' (Meghini et al. 2019, Borrego et al., 2019, Ragot et al., 2017 en Ollander et al., 2016).

Om de validiteit van de metingen met de Empatica E4 en vergelijkbare wearables op een goede manier te kunnen testen en beoordelen hebben Van Lier et al. (2019) een uitgebreid protocol ontwikkeld. Dit gestandaardiseerde protocol test de validiteit op drie verschillende niveaus. Dit zijn het signaalniveau, oftewel de ruwe gegevens zoals het patroon in een ecg- of PPG-grafiek, het parameterniveau, oftewel geaggregeerde gegevens zoals gemiddelde hartslag, en het niveau van reacties op gebeurtenissen, bijvoorbeeld fysiologische reacties op een stresstaak. De eerste resultaten van dit protocol met de Empatica E4 laten zien dat zowel hartslag als huidgeleiding valide gemeten wordt, zowel op parameter- als op gebeurtenisniveau. Daarbij wordt waar het huidgeleiding betreft wel opgemerkt dat de Empatica E4 alleen gebruikt zou moeten worden bij het meten van de fysiologische effecten van relatief sterke en langdurige stressoren. Lichte, kortstondige stressoren worden niet goed gedetecteerd. Dit is in lijn met de bevindingen van een andere studie die het gebruik van de Empatica E4 bij neutrale en te lichte emotionele stimuli afraadt (Borrego et al., 2019).

3 Dataveiligheid en privacy bij gebruik van de Empatica E4

3.1 Inleiding

In dit hoofdstuk wordt voor de Empatica E4 onderzocht wat er vanuit de fabrikant bekend is over de opslag van de fysiologische gegevens (paragraaf 3.2), het transport van deze gegevens (paragraaf 3.3), de toegang tot deze gegevens (paragraaf 3.4), en de manier waarop de privacy van de gegevens gewaarborgd wordt (paragraaf 3.5). Het betreft hier steeds de door de gebruiker (in de justitiële context vaak een onderzoeker, behandelaar of toezichthouder) verzamelde fysiologische gegevens van de drager van de polsband (in de justitiële context vaak een justitiabele). Vervolgens bespreken we in paragraaf 3.6 aan de hand van de gevonden informatie, welke risico's we zien wat betreft de veiligheid van de fysiologische gegevens en de privacy van de drager.

3.2 Gegevensverzameling en -opslag

Figuur 10 Verschillende plaatsen waar fysiologische gegevens (tijdelijk) opgeslagen worden

Bron: aangepast van https://e4.empatica.com

De fysiologische gegevens worden op verschillende plekken (tijdelijk) opgeslagen (zie figuur 10): op de polsband zelf, op het mobiele apparaat en/of de computer van de gebruiker (externe apparaten), en in de cloud (E4 Connect). Deze drie locaties worden hieronder één-voor- één besproken. Daarbij wordt steeds aangegeven 1) wat er precies wordt opgeslagen, 2) wanneer deze opslag plaatsvindt en 3) welke beveiligingsmaatregelen er zijn genomen ten aanzien van de opslag.

3.2.1 Op de polsband zelf

In de opnamemodus (in figuur 10 gemarkeerd met een 1) worden de gegevens van de vier sensoren eerst op de polsband zelf opgeslagen. Een sessie blijft opgeslagen

op de polsband totdat deze met succes is overgezet naar een lokale computer. De gegevens worden ook niet gewist als de polsband wordt gereset of als deze de stroom verliest. Het geheugen wordt pas gewist na een succesvolle overdracht via de *E4 Manager*-software op de lokale computer (dit gebeurt dan automatisch). In totaal kan de polsband tot 36 uur aan sessies opslaan in het flash geheugen. Als het geheugen vol is, stopt de Empatica E4 met opnemen.

De gegevens kunnen niet eenvoudig handmatig door de gebruiker van de polsband gewist worden. De gebruiker kan de gegevens alleen van de polsband verwijderen door ze over te zetten naar een ander apparaat. Andersom kan de gebruiker het wissen van gegevens op de polsband ook niet voorkomen bij het overzetten naar een ander apparaat omdat dit automatisch gaat.

De gebruiker kan ook niet zelf bepalen *welke* gegevens worden opgeslagen: 60 seconden nadat de band wordt aangezet, begint de band met opnemen en worden de metingen van alle aanwezige sensoren verzameld en opgeslagen. Het is geen standaardfunctionaliteit om (een of meerdere) sensoren uit te schakelen. Het is wel mogelijk om een van de sensoren aan de buitenkant af te plakken, zodat er geen metingen geregistreerd worden.

De gegevens op de polsband zijn beveiligd doordat ze zijn opgeslagen in een *custom* binair formaat[32] (een zogenoemde *protection through obscurity*). Dit formaat kan niet geïnterpreteerd worden zonder gebruik te maken van de *application programming interface* (API)[33] van Empatica. Het is echter niet uit te sluiten dat bestanden in dit formaat door hackers met de juiste kennis en vaardigheden gekraakt kunnen worden. De kans hierop wordt groter als de hacker toegang heeft tot een grote hoeveelheid data(bestanden) in het betreffende formaat.

3.2.2 Op externe apparaten

In de streamingmodus (in figuur 10 gemarkeerd met een 2) worden de gegevens niet eerst op de polsband zelf opgeslagen, maar worden ze direct (in real time) getoond in de app op het mobiele apparaat. Ook in deze modus kan de gebruiker niet zelf bepalen van welke sensoren de metingen worden getoond. Het is ons onbekend of de gegevens ook lokaal op het mobiele apparaat worden opgeslagen en wanneer deze gewist (kunnen) worden. Dit kon door ons niet achterhaald worden.

In de opnamemodus (in figuur 10 gemarkeerd met een 1) worden de gegevens van een sessie die op de polsband staan na verbinding met USB en het opstarten van *E4 manager* eerst automatisch verplaatst naar een tijdelijke opslag op een computer.

---

[32] Een bestand in binair formaat is een computerbestand dat volledig uit bitcombinaties bestaat. Meestal bevat een binair bestand reeksen van bytes die bestaan uit acht bits. Vaak zijn dit bytes die niet als tekstkarakters geïnterpreteerd moeten en kunnen worden. In een tekstbestand daarentegen komen alleen bitcombinaties voor die corresponderen met leesbare tekens (letters en cijfers). In een binair bestand zijn de bytes op zichzelf betekenisloos. Er is altijd een computerprogramma nodig om het bestand te kunnen lezen en weergeven. Voor standaard binaire bestanden (bijvoorbeeld ASCII-tekst of JPEG-foto's) bestaan veel verschillende van zulke programma's. Een bestand in een custom binair formaat gaat niet uit van een standaardformaat, daarom is het bestand alleen leesbaar in een specifiek computerprogramma.

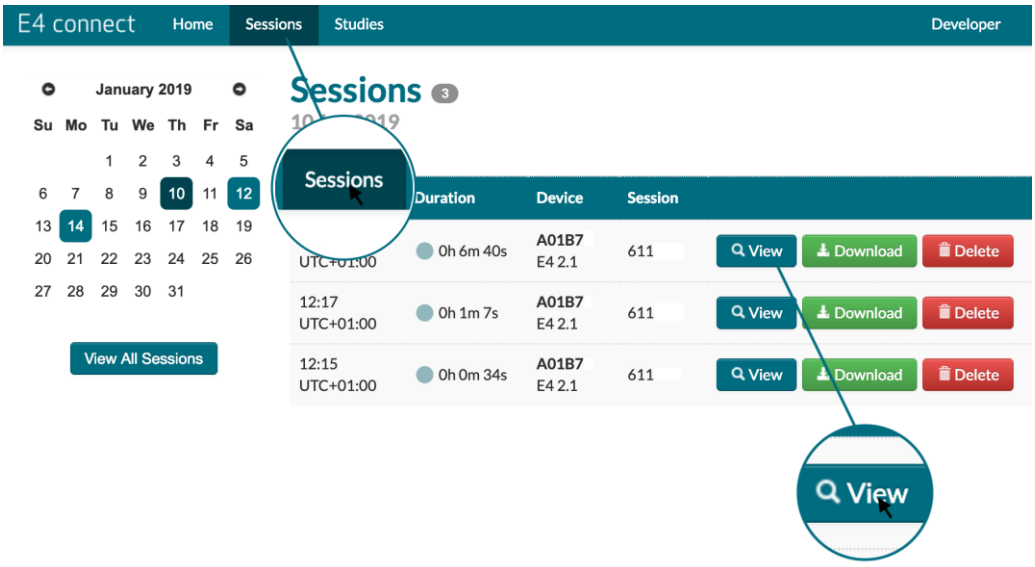
[33] Een API is een set aan definities waarmee verschillende softwareapplicaties of -systemen met elkaar kunnen communiceren en informatie kunnen uitwisselen. Het dient als een interface tussen verschillende applicaties zodat toegang tot informatie of functionaliteiten automatisch geregeld is, zonder dat ontwikkelaars hoeven te weten hoe het andere programma exact werkt.

Deze blijven daar staan totdat ze zijn geüpload naar *E4 Connect*. Lokale bestanden worden dus nooit verwijderd voordat ze worden geüpload. Nadat de gegevens met succes zijn geüpload naar *E4 Connect*, worden deze gearchiveerd op de computer. Het is bij ons onbekend hoe en waar dit precies gebeurt en het is ook onbekend of dit archief (handmatig) verwijderd kan worden.

3.2.3 In de cloud

Ongeacht de gekozen modus worden de gegevens uiteindelijk altijd in de cloud opgeslagen (in dit geval Empatica's *E4 Connect*, in figuur 10 gemarkeerd met een 3). Dit gebeurt ook steeds automatisch als het mobiele apparaat of de computer verbinding maakt met het internet. Hier heeft de gebruiker geen invloed op. Het online platform biedt, naast opslagcapaciteit, een API voor het betekenisvol bekijken en interpreteren van de gegevens. Dit wordt door Empatica genoemd als beveiligingsmaatregel, maar zorgt er tegelijkertijd voor dat de gegevens bijna altijd via het internet moeten worden verstuurd naar Empatica en dat het, zonder zelf een app te ontwikkelen, niet mogelijk is de polsband alleen lokaal te gebruiken. Het is hierbij wel zo dat de gegevens in *E4 Connect* alleen zijn gelinkt aan de gebruiker en niet per se (direct) aan de persoon die de polsband draagt. Dit heeft als voordeel dat het lastiger is de fysiologische gegevens te koppelen aan de betreffende persoon.

Figuur 11 Mogelijkheden om de verzamelde fysiologische gegevens te beheren op de E4 Connect-website



Op de *E4* Connect-website zijn er voor de gebruiker mogelijkheden om de opgeslagen gegevens te beheren (zie Figuur 11). Zo kunnen de onbewerkte gegevens in CSV-indeling[34] gedownload worden zodat ze in andere toepassingen verder verwerkt of geanalyseerd kunnen worden. De gegevens zijn dan wel gewoon leesbaar zonder API. De gebruiker is na deze download zelf verantwoordelijk voor de opslag en beveiliging. Een andere mogelijkheid is om de gegevens uit het account van de gebruiker te verwijderen. Alleen in *E4 Connect* heeft de gebruiker dus enige eigen invloed

[34] CSV staat voor *comma seperated values*. Dit is een specificatie voor tabelbestanden. De kolommen in het bestand worden gescheiden door een komma.

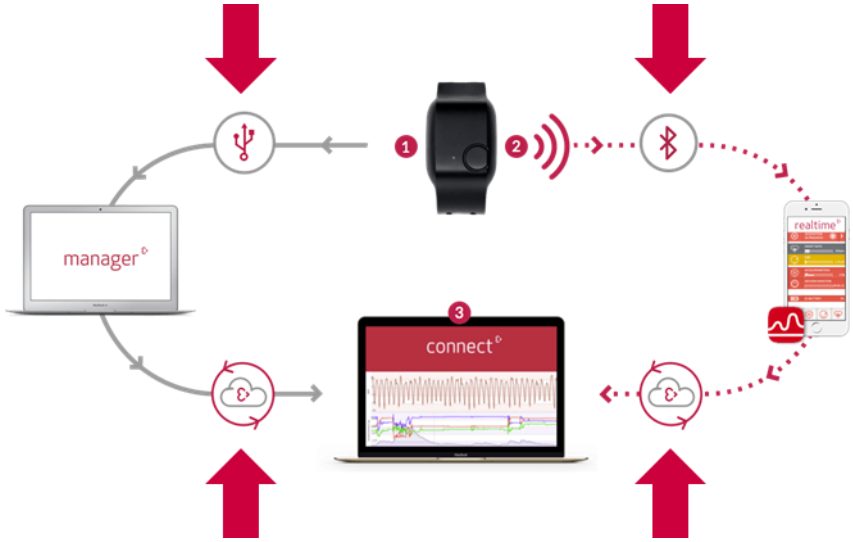
op welke gegevens er bij Empatica opgeslagen, bewaard en verwijderd worden. Het verwijderen van gegevens gaat steeds per sessie. Het lijkt erop dat Empatica deze sessie daarna nog wel bewaart (maar dan niet meer gekoppeld aan een specifiek account van een gebruiker).

De online opslag van de gegevens in *E4 Connect* wordt gehost bij *Amazon Web Services* (AWS) dat ISO 27001 (voor procesmatige informatiebeveiliging) en SOC 3 (voor hosting en datacenters) gecertificeerd is. AWS heeft meerdere datacenters, zowel binnen als buiten de EU.[35] Het is ons onbekend in welk datacenter en in welk land de gegevens van Empatica precies worden opgeslagen.

Empatica heeft op de website en in de privacyverklaring niet gespecificeerd wat de bewaartermijn van de verzamelde fysiologische gegevens is. Na navraag van onze kant (zie bijlage 3), schrijft Empatica daarover: '*Given the sensitivity of the clients we deal with, often we sign separate agreements that supersede the privacy policy: for example, with pharmaceutical companies or government agencies, we agree to separate terms that might have different requirements for retention policies, data access, audit rights, confidentiality etc.*'

3.3 Gegevenstransport

Figuur 12 Verschillende manieren waarop de verzamelde fysiologische gegevens uitgewisseld worden



Bron: aangepast van https://e4.empatica.com

In deze paragraaf wordt beschreven op welke manier de verzamelde fysiologische gegevens uitgewisseld worden tussen de verschillende opslagmodi (polsband, mobiel apparaat/computer en cloud, zie figuur 12). Er wordt beschreven 1) welke gegevens worden verzonden, 2) wanneer dit gebeurt en 3) welke beveiligingsmaatregelen daarbij zijn genomen.

[35] https://aws.amazon.com/about-aws/global-infrastructure

Het datatransport naar *E4 Connect* vindt altijd plaats via de computer of het mobiele apparaat van de gebruiker, omdat de polsband zelf niet de mogelijkheid heeft om verbinding te maken met het internet. In de streamingmodus worden de gegevens verzonden van de Empatica E4 naar de app via bluetooth en vervolgens automatisch van de app naar Empatica via de internetverbinding van het mobiele apparaat (wifi of 3G/4G). In de opnamemodus is de verbinding tussen Empatica E4 en computer via USB. Het transport van de computer naar de cloud gaat automatisch en via de internetverbinding van de computer (dit kan zowel draadloos als bedraad zijn).

Als er nieuwe metingen gedaan zijn, vindt transport van gegevens plaats telkens wanneer er een internetverbinding is. De gebruiker kan het verzenden van gegevens alleen pauzeren door de internetverbinding te verbreken. Zodra er weer verbinding wordt gemaakt, wordt het verzenden automatisch hervat. De gebruiker kan dus bijna niet voorkomen dat de gegevens naar de cloud verzonden worden. Daarnaast kan de gebruiker niet kiezen welke gegevens verzonden worden. Dit is altijd een gehele sessie en alle metingen in een sessie. Net zoals bij de opslag heeft de gebruiker weinig eigen invloed op het gegevenstransport. Pas achteraf, als de gegevens al verzonden zijn, kan de gebruiker via de *E4 Connect*-website gegevens (laten) wissen uit het account.

Zowel verbindingen via USB als bluetooth gelden als behoorlijk veilig. Apparaten die gebruikmaken van bluetooth[36] moeten dicht bij elkaar in de buurt zijn om gegevens uit te kunnen wisselen, meestal binnen een afstand van tien meter. Wanneer een apparaat voor het eerst met een ander apparaat verbindt, moet de nieuwe verbinding eerst goedgekeurd worden. Door beide aspecten is het moeilijk het signaal te onderscheppen en gegevens te stelen. Informatie-uitwisseling via bluetooth is veiliger dan via internet, maar er zijn kwetsbaarheden die hackers kunnen misbruiken. Om gegevens te kunnen stelen moet een hacker wel bij de locatie van beide apparaten in de buurt zijn. Om het risico nog verder te verkleinen is het van belang om alleen apparaten die up-to-date zijn en de laatste beveiligingsupdates geïnstalleerd hebben met elkaar te verbinden. Een verbinding via USB[37] is altijd bedraad en daarom over het algemeen nog veiliger dan een verbinding via bluetooth. Voor hackers is het onmogelijk om deze gegevensoverdracht te onderscheppen. Het verzenden van gegevens via internetverbindingen is het onveiligst, hiervoor zijn aanvullende beveiligingsmaatregelen nodig.

De verbinding met *E4 Connect* (de verbinding met de servers van Empatica voor zowel het uploaden als downloaden van gegevens, de onderste twee pijlen in figuur 12) is met 128 bits versleuteld (SHA-256,[38] TLS 1.2[39]). Dit zorgt ervoor dat de gegevens gecodeerd verstuurd worden en dat alleen met de juiste sleutel de originele gegevens weer ontcijferd kunnen worden. Het aantal bits bepaalt hoe sterk er versleuteld wordt. Hoe meer bits, hoe lastiger het is om de sleutel te kraken. Een beveiliging met meer bits is daardoor sterker. Voor communicatie tussen computers

[36] Bluetooth is een open standaard voor draadloze (radio)verbindingen tussen apparaten op korte afstand en kan worden gebruikt om apparaten met elkaar te laten communiceren en bestanden uit te wisselen.

[37] USB is een afkorting van *universal serial bus* en kan gebruikt worden voor het aansluiten van randapparatuur op computers en snelle gegevensoverdracht. Het aansluiten van apparatuur gaat via een kabel.

[38] SHA staat voor *Secure Hash Algorithm.* Dit is een cryptografische functie waarmee gegevens gepseudonimiseerd kunnen worden.

[39] TLS staat voor *Transport Layer Security*. Dit is een encryptieprotocol voor het beveiligen van communicatie op het internet.

is 128-bitsversleuteling nu nog de norm (dit wordt als veilig beschouwd; de hoeveelheid vereiste rekenkracht voor het kraken van deze versleuteling ligt ver boven de mogelijkheden van de huidige snelste computers), maar 256-bitencryptie is in opkomst. Als extra veiligheidsmaatregel worden de gegevens ook nog verzonden in een niet-standaard formaat. Hierdoor is het transport onderscheppen alleen niet voldoende om de fysiologische gegevens te kunnen lezen. De onderschepper moet de gegevens dan eerst ontsleutelen en heeft vervolgens ook nog toegang tot de API van Empatica nodig om de gegevens te kunnen begrijpen.

Deze API is alleen te bevragen met een geldige (ontwikkelaars)sleutel (een *Empatica API key*) die alleen ter beschikking wordt gesteld aan gebruikers die apps willen ontwikkelen (ontwikkelaars). Iedere gebruiker met een *E4 Connect*-account kan echter ontwikkelaar worden en dus een sleutel krijgen. Met een dergelijke sleutel kunnen in principe alleen polsbanden die zijn gekoppeld aan het account van de gebruiker/ontwikkelaar gebruikt worden. Hiertoe moet eerst de unieke aankoopcode die bij de polsband hoort (die wordt door Empatica in de verzendbevestiging opgenomen), geregistreerd worden. Het is dus niet zomaar mogelijk om met deze sleutel de API te gebruiken voor willekeurige onderschepte gegevens. Het is ons echter onbekend hoe (goed) Empatica (toegang tot en gebruik van) deze API beveiligd heeft tegen bijvoorbeeld hacken.

Door gebruik te maken van een zelfontwikkelde app of een app van derden (zie paragraaf 2.3.4) is het mogelijk om het verzenden van gegevens naar Empatica te voorkomen. De gegevens worden dan via bluetooth naar het gekoppelde mobiele apparaat verstuurd. Afhankelijk van de app worden de gegevens vervolgens lokaal opgeslagen en/of naar een andere cloudprovider gestuurd.

3.4 Toegang tot gegevens

Figuur 13 Toegang tot de verzamelde fysiologische gegevens via E4 Connect

Bron: aangepast van https://e4.empatica.com

De gebruiker kan toegang krijgen tot de bij Empatica opgeslagen fysiologische gegevens via de *E4 Connect*-website (in figuur 13 gemarkeerd met een 3). De gegevens zijn toegankelijk via de grafische gebruikersinterface (GUI) van deze

webapplicatie. De gebruiker kan, zoals eerder beschreven, vanuit deze applicatie de gegevens downloaden naar de eigen computer.

De gebruiker krijgt toegang tot de gegevens in het account door zich te identificeren met een emailadres en wachtwoord. Hierbij valt op dat Empatica geen eisen stelt aan het gekozen wachtwoord. Ook een wachtwoord bestaande uit één letter wordt geaccepteerd bij het aanmaken van een account. Daarnaast zijn er geen extra beveiligingsmaatregelen genomen zoals twee-factor-authenticatie.[40]

Omdat hierover op de website onvoldoende informatie aanwezig was, en de privacyverklaring niet over de fysiologische gegevens gaat, is bij Empatica navraag gedaan met betrekking tot de toegang tot en het gebruik van de fysiologische gegevens door Empatica zelf en door andere partijen (zie bijlage 3). Empatica schrijft hierover: *'As a matter of internal procedures and quality standards, a more stringent access policy is applied to the data collected by the E4. Specifically, only authorized technical professionals employed by Empatica can access the data, in the case of support/troubleshooting, or when requested by the Client for reasons beyond support/troubleshooting (for example, if the client asks Empatica to perform data analytics on the data).'* In paragraaf 3.2 is al beschreven dat het mogelijk is een overeenkomst met Empatica af te sluiten, waarin hierover aanvullende afspraken gemaakt worden.

3.5 Privacy van de gegevens

Zoals uitgelegd in paragraaf 1.3 is op de verwerking van persoonsgegevens in de justitiële context de AVG of de richtlijn gegevensbescherming opsporing en vervolging (voor Nederland uitgewerkt in de Wjsg) van toepassing. Aanvullend kunnen ook andere wetten van toepassing zijn en bepalen welke grondslag voor de gegevensverwerkingen geldt.

Gegevens zijn persoonsgegevens als ze direct over iemand gaan of naar deze persoon te herleiden zijn. Hierbij is het van belang onderscheid te maken tussen gepseudonimiseerde en anonieme gegevens. Bij pseudonimiseren wordt de identiteit van een persoon verhuld voor derden door (direct) identificerende gegevens te vervangen door versleutelde gegevens (pseudoniemen). Zo kan de naam van de drager van een wearable worden vervangen door een uniek nummer. Alleen de gebruiker kan dan nog achterhalen welke gegevens bij welke persoon horen. Gepseudonimiseerde gegevens zijn niet anoniem, omdat er een koppeling tot stand kan worden gebracht tussen de gepseudonimiseerde gegevens en identificerende gegevens. Het gaat hier daarom nog steeds om persoonsgegevens waarop de AVG of Wjsg van toepassing is. Pseudonimisering is volgens de AVG wel een goede maatregel om persoonsgegevens te beschermen en te beveiligen. Anonieme gegevens zijn gegevens die niet terug te voeren zijn naar een identificeerbare natuurlijke persoon, ook niet door herleiding, koppeling of deductie. Hierop is de AVG of Wjsg niet (meer) van toepassing.

Een eerder onderzoek van het WODC (Bargh et al., 2018) heeft laten zien dat het heel lastig is om gegevens zodanig te bewerken dat een dataset volledig anoniem

[40] Hierbij is naast een wachtwoord nog een tweede factor nodig om in te kunnen loggen (de identiteit van de gebruiker wordt dan door middel van twee factoren vastgesteld). Dit kan bijvoorbeeld een code zijn die per sms wordt verstuurd of een vingerafdruk. Dit is een veiligere manier van inloggen dan alleen een wachtwoord.

wordt en op geen enkele manier meer tot personen te herleiden is. De anonimiteit van gegevens hangt bijvoorbeeld samen met de motivatie van een kwaadwillende voor het identificeren van (een of meerdere) de personen in een dataset, de voor hem/haar beschikbare technologieën en de aanwezigheid van andere gegevensbronnen over de personen in de dataset. Specifiek in de context van wearables stelt de Article 29 Data Protection Working Party (2017) van de Europese Commissie, inmiddels European Data Protection Board (EDPB) genaamd hetzelfde: '*It is technically very difficult to ensure complete anonymisation of the data*' (p. 18). Deze uitspraak gaat weliswaar over wearables op de werkvloer, maar kan ook worden doorgetrokken naar gebruik in de justitiële context. Dat een fysiologisch gegeven, zoals hartslag, heel persoonlijk en uniek kan zijn, blijkt wel uit een toepassing die door het Amerikaanse ministerie van Defensie ontwikkeld is. De ontwikkelde infraroodlaser kan op een afstand van 200 meter personen herkennen aan hun hartslag.[41]

Dit in acht nemend, kan gesteld worden dat de fysiologische gegevens die verzameld worden van de drager van een wearable persoonsgegevens zijn. Voor de gebruiker zijn de gegevens van de dragers sowieso in bijna alle gevallen te herleiden tot personen. Als met de wearable fysiologische gegevens verzameld worden die over iemands gezondheid gaan, is sprake van bijzondere persoonsgegevens die nog eens extra beschermd dienen te worden (zie artikel 9 van de AVG). Met deze gegevens moet daarom zorgvuldig omgegaan worden, conform de op het gebruik van toepassing zijnde (privacy)wetgeving (dit kan naast de AVG of Wjsg bijvoorbeeld ook de WGBO zijn), om de privacy van de drager niet te schaden.

Bij het uitvoeren van wetenschappelijk onderzoek met fysiologische gegevens, maar ook bij het behandelen van patiënten op basis van fysiologische gegevens of het houden van toezicht met behulp van fysiologische gegevens, moet de onderzoeker, de behandelaar of de toezichthouder (of het instituut waaraan zij verbonden zijn) als de zogenoemde *verwerkingsverantwoordelijke* voldoen aan de op het gebruik van toepassing zijnde privacywetgeving. Het is dan onder meer nodig om de verwerkingen bij te houden in een verwerkingsregister. Als de verwerking een hoog privacyrisico oplevert, is het daarnaast verplicht om een *Data Protection Impact Assessment* (DPIA)[42] uit te voeren waarin deze risico's vooraf in kaart gebracht worden. Een DPIA is onder andere verplicht als er op grote schaal bijzondere persoonsgegevens worden verwerkt. In sommige gevallen, bijvoorbeeld als wetenschappelijk onderzoek wordt uitgevoerd, kan het om aan de (privacy)wetgeving te voldoen aanvullend nodig zijn om de dragers van de wearable te informeren over de voorgenomen verwerking en toestemming te vragen voor deze verwerking (zodat er een grondslag voor de verwerking ontstaat).[43]

De verwerkingsverantwoordelijke (in dit geval de gebruiker) heeft in de privacywetgeving een verantwoordingsplicht en moet kunnen aantonen dat de juiste technische en organisatorische maatregelen zijn genomen om de verzamelde

---

[41] www.technologyreview.com/2019/06/27/238884/the-pentagon-has-a-laser-that-can-identify-people-from-a-distanceby-their-heartbeat/

[42] In het Nederlands wordt dit ook wel een gegevensbeschermingseffectbeoordeling, afgekort GEB, genoemd.

[43] Deze grondslag voor het verwerken van persoonsgegevens zal in het zorg- of veiligheidsdomein nauwelijks een rol spelen, omdat er door de afhankelijkheidsrelatie van vrije toestemming vaak geen sprake zal zijn. Vaak geldt in deze domeinen een andere grondslag voor de verwerking. In de zorg gaat de zorgverlener met de patiënt bijvoorbeeld een geneeskundige behandelovereenkomst aan die onder de WGBO valt. Deze overeenkomst is de grondslag voor de gegevensverwerkingen en aparte toestemming is niet nodig. Als de gegevens voor andere doelen dan voor de behandeling worden verwerkt, dan kan aanvullende toestemming overigens wel nodig zijn.

gegevens te beveiligen. Dit kan door maatregelen te nemen en toe te passen die voldoen aan het beginsel van gegevensbescherming door ontwerp (*privacy by design*). Dit houdt in dat er al in het voortraject (bijvoorbeeld bij het opzetten van het onderzoek) aandacht is voor privacy en privacyverhogende maatregelen (ook wel *privacy enhancing technologies* genoemd). Ook het vooraf nadenken over welke gegevens er echt nodig zijn en het verwerken van zo min mogelijk persoonsgegevens (dataminimalisatie) is hier onderdeel van. Daarnaast kan de gebruiker zorgen voor privacybeschermende instellingen (*privacy by default*).

Bij de Empatica E4 wordt gebruikgemaakt van de cloud: de fysiologische gegevens worden opgeslagen op de server van de Empatica bij Amazon Web Services. Er is dan een externe partij betrokken bij de verwerking van deze gegevens. Deze partij wordt in de privacywetgeving de verwerker genoemd. Ook de cloudprovider moet voldoen aan de privacywetgeving. De juridische eisen aan en risico's van de opslag van medische data in de cloud staan in een recent advies van ICTRecht (2019). Naast het voldoen aan de AVG is het bijvoorbeeld ook belangrijk dat het medisch beroepsgeheim zoals vastgelegd in de WGBO gewaarborgd wordt.

De verwerkingsverantwoordelijke blijft verantwoordelijk en dient te controleren of de verwerker ook daadwerkelijk aan de privacywetgeving voldoet. Ook moet de verwerkingsverantwoordelijke een verwerkersovereenkomst afsluiten met de verwerker, waarin onder andere afspraken worden vastgelegd over de (technische en organisatorische) bescherming van de te verwerken persoonsgegevens. Het niet opslaan van direct identificerende gegevens over de drager is een voorbeeld van een beschermingsmaatregel die genomen kan worden door de verwerker. Dit is een maatregel die Empatica ook genomen heeft. Omdat de AVG de inhoud van een verwerkersovereenkomst in grote mate voorschrijft, zijn er diverse standaardmodellen ontwikkeld. Binnen de Rijksoverheid is dit bijvoorbeeld het ARVODI-model.[44] Ook voor de zorg is er een modelverwerkersovereenkomst.[45]

Bij het gebruik van clouddiensten is het daarnaast belangrijk om er rekening mee te houden dat op de gegevensverwerking meerdere rechtsregimes van toepassing kunnen zijn.[46] Zo kunnen gegevens (wellicht ongemerkt) terecht komen in een land buiten de EU waar mogelijk de wettelijke bescherming van gegevens onvoldoende is geregeld. Als de gegevens bijvoorbeeld op een server in de Verenigde Staten worden opgeslagen, kan de CLOUD Act (*Clarifying Lawful Overseas Use of Data Act*) Amerikaanse autoriteiten toegang geven tot persoonsgegevens. Het doorgeven van gegevens vanuit de EU naar landen daarbuiten mag volgens de AVG niet zomaar (zie artikel 44). Er moet dan sprake zijn van een passend beschermingsniveau (een adequaatheidsbeslissing)[47] of passende waarborgen om de betrokkenen te beschermen. Een passende waarborg is bijvoorbeeld een modelcontractbepaling die door de Europese Commissie is vastgesteld.

---

[44] www.pianoo.nl/nl/document/9596/model-verwerkersovereenkomst-arvodi

[45] www.brancheorganisatieszorg.nl/nieuws_list/modelverwerkersovereenkomst-voor-de-zorgsector/

[46] Zoals uitgewerkt in het Cloud PIA Model van de Directie Informatievoorziening & Inkoop (DI&I) dat een cloud-specifieke toelichting geeft bij het Model gegevensbeschermingseffectbeoordeling Rijksdienst (PIA) en het advies van ICTRecht (2019).

[47] Voorheen was de uitwisseling van persoonsgegevens tussen de EU en de VS geregeld in het *privacy shield*. Het Hof van Justitie van de EU heeft het EU-VS privacy shield op 16 juli 2020 echter ongeldig verklaard (European Data Protection Board, 2020b). Dit betekent dat geen persoonsgegevens aan de VS meer kunnen worden doorgeven op grond van het privacy shield. De EDPB bekijkt wat de praktische gevolgen zijn van de uitspraak.

Empatica heeft aangegeven dat met overheidsinstanties vaak aparte overeenkomsten worden afgesloten, waarin aanvullende afspraken worden gemaakt met betrekking tot de toegang tot de data, de bewaartermijnen en vertrouwelijkheid. '*Given the varying requirements on how our products are used, these agreement are generally custom contracts and vary in the specifics'*. Hierin is dus maatwerk mogelijk. Het is niet onderzocht in hoeverre de overeenkomst die Empatica aanbiedt voldoende waarborgen biedt om aan de geldende privacywetgeving te voldoen.

Als de Empatica E4 gebruikt wordt in de justitiële context is het volgende nodig om aan de privacywetgeving te kunnen voldoen:

- De gebruiker kan als verwerkingsverantwoordelijke de naleving van de privacywetgeving aantonen door onder andere een verwerkingsregister bij te houden, vooraf een DPIA uit te voeren, en passende technische en organisatorische maatregelen te nemen (*privacy by design)*.
- Er is een verwerkersovereenkomst tussen Empatica en gebruiker waarin onder meer afspraken worden gemaakt (die in lijn zijn met de privacywetgeving) over de opslag, toegang, bewaartermijnen en (her)gebruik van de fysiologische gegevens en eventueel andere persoonsgegevens (bijvoorbeeld: opslag bij voorkeur binnen de EU);
- Als er geen andere wettelijke grondslag voor de verwerking van de gegevens is (bijvoorbeeld het uitvoeren van een wettelijke verplichting of taak) of bij het uitvoeren van medisch-wetenschappelijk onderzoek dat onder de WMO valt:
  - De gebruiker heeft toestemming van de dragers voor het verzamelen van hun fysiologische gegevens (*informed consent*);
  - De dragers hebben vrijelijk kunnen beslissen over het geven van toestemming.

3.6 Samenvatting en discussie: belangrijkste veiligheids- en privacy-risico's

Empatica heeft verschillende maatregelen genomen om de fysiologische gegevens van de dragers tijdens transport en opslag op de servers van Empatica te beveiligen tegen het eventuele onderscheppen ervan door derden. Zo worden de gegevens gekoppeld aan de gebruiker en niet aan de drager, opgeslagen in een speciaal formaat, en versleuteld verzonden. Desondanks zijn er een aantal risico's op het gebied van veiligheid en privacy. Deze zijn samengevat in figuur 14.

Figuur 14 Overzicht van de belangrijkste veiligheids- en privacyrisico's bij het gebruik van de Empatica E4

Bron: aangepast van https://e4.empatica.com

Figuur 14 laat zien dat er met betrekking tot de veiligheid op verschillende plekken risico's zijn (gemarkeerd met de uitroeptekens); zowel bij de opslag als het transport van de fysiologische gegevens. Het voornaamste risico van de Empatica E4 dat de gebruiker weinig invloed heeft op wat er wanneer naar de cloud wordt verstuurd en dat het niet eenvoudig mogelijk is de polsband geheel lokaal te gebruiken (dit kan alleen als er een eigen app ontwikkeld wordt). Gegevens verzenden via internet en opslaan op een cloudserver introduceert een potentiële kwetsbaarheid en maakt het mogelijk om gegevens te onderscheppen of stelen zonder dat een kwaadwillende fysieke toegang tot de wearable zelf heeft. Bij lokaal gebruik, waarbij gebruikgemaakt wordt van een USB- en/of bluetoothverbinding is dit risico een stuk kleiner. De cloud van Empatica is daarnaast matig beveiligd met alleen een wachtwoord, waardoor de kans op succesvol hacken groter is. De beveiligingsmaatregel dat de fysiologische gegevens zonder de API van Empatica in principe onleesbaar zijn, zorgt er tegelijkertijd voor dat de gegevens altijd via het internet moeten worden verstuurd.

Aan de andere kant is de wens om voor een cloudoplossing te kiezen vanuit de gebruiker goed te begrijpen (ICTRecht, 2019). Cloudproviders bieden over het algemeen mogelijkheden voor de verwerking en bescherming van gegevens die voor gebruikers niet altijd goed te realiseren zijn (bijvoorbeeld doordat zij daarvoor niet de juiste expertise of middelen hebben). Cloudproviders hebben (bedrijfs)belang bij het aanbieden van zo betrouwbaar en veilig mogelijke systemen voor de opslag en verwerking van gegevens. Ze zijn hierin gespecialiseerd en kunnen gebruikmaken van schaalvoordelen. Het kiezen van een goed beveiligde cloudprovider kan een gebruiker helpen bij het nakomen van de wettelijke verplichting tot het beschermen van de verzamelde fysiologische gegevens.

Dit brengt ons bij de belangrijkste aandachtspunt op het gebied van de privacy van de drager van de Empatica E4 (gemarkeerd met het slotje in figuur 14). De fysiologische gegevens die verzameld worden met de Empatica E4 zijn persoonsgegevens die conform de privacywetgeving zorgvuldig behandeld moeten worden. Er is hier bovendien sprake van bijzondere persoonsgegevens die over iemands gezondheid gaan en die daarom extra beschermd dienen te worden. Op de stelling van Empatica dat de verzamelde fysiologische gegevens effectief anoniem zijn valt onzes inziens het een en ander af te dingen. Onderzoek laat zien dat het heel lastig is om gegevens zodanig te bewerken dat een dataset volledig anoniem wordt en op geen enkele manier meer tot personen te herleiden is. Ook Empatica, als verwerker van de verzamelde gegevens, moet daarom voldoen aan de privacywetgeving. Het is conform deze wetgeving verplicht om een verwerkersovereenkomst met Empatica af te sluiten, waarin duidelijke afspraken worden gemaakt over wat er met de gegevens gebeurt, en wie er toegang toe heeft. Hoewel Empatica aangeeft met verschillende partijen toegespitste overeenkomsten af te sluiten, is hier niet onderzocht in hoeverre deze overeenkomsten voldoende waarborgen bieden.

4 Vergelijking: functionaliteit, dataveiligheid en privacy van andere wearables geschikt voor onderzoek, behandeling en toezicht

4.1 Inleiding

Naast de Empatica E4 van Empatica zijn er nog andere wearables beschikbaar die ingezet zouden kunnen worden voor onderzoek, behandeling en toezicht in de justitiële context. Zo biedt Empatica naast de E4 nog twee andere producten voor klinische studies. Daarnaast zijn er verschillende andere fabrikanten die wearables voor onderzoeksdoeleinden of behandeling door zorgprofessionals aanbieden, en zijn
er op de consumentenmarkt vele producten beschikbaar die ook voor onderzoek of behandeling ingezet zouden kunnen worden. In dit hoofdstuk beschrijven we een aantal van deze wearables. Hierbij kijken we naar de belangrijkste verschillen vergeleken met de Empatica E4, vooral met betrekking tot dataveiligheid en privacy. Bij onze selectie van de te bespreken wearables hebben we vooral instrumenten uitgekozen die op het gebied van de sensoren lijken op de Empatica E4 en/of in ieder geval huidgeleiding meten, of die wijdverspreid gebruikt worden. Er zijn naast de hier genoemde wearables, nog veel meer producten voor professioneel en/of consumentengebruik beschikbaar die geen EDA-sensor voor huidgeleiding, maar bijvoorbeeld wel een ecg-sensor bevatten (zie voor een overzicht Taj-Eldin et al., 2018, Cosoli et al., 2020 en Saganowski et al., 2020). Het overzicht in dit hoofdstuk is mogelijk niet compleet en heeft vooral als doel om te laten zien in hoeverre de Empatica E4 verschilt van andere wearables die geschikt zouden kunnen zijn voor gebruik in de justitiële context en om daarmee de voor- en nadelen van de Empatica E4 ten opzichte van andere producten in kaart te brengen.

In paragraaf 4.2 bespreken we eerst de andere wearables die Empatica aanbiedt. Vervolgens bespreken we in paragraaf 4.3 wearables die gericht zijn op gebruik door professionals tijdens onderzoek of in de zorg en in paragraaf 4.4 wearables voor de consumentenmarkt. In paragraaf 4.5 vergelijken we deze wearables vervolgens met de Empatica E4.

4.2 Wearables van Empatica

Naast de E4 biedt Empatica nog twee andere polsbanden voor onderzoeksdoeleinden aan: *Embrace2* en *EmbracePlus*. De Embrace2[48] is vooral gericht op gebruik in de zorg, het instrument is bedoeld voor patiënten met epilepsie en kan (zorgverleners) waarschuwen bij mogelijke aanvallen, maar kan ook ingezet worden voor klinisch onderzoek. Deze polsband bevat net als de E4 vier sensoren, maar bevat in plaats van een hartslagmeter een gyroscoop (een bewegings- en versnellingsmeter). Deze polsband kan tevens gebruikt worden voor onderzoek, maar daarvoor is wel een aanvullend abonnement nodig om de (ruwe) gegevens te kunnen exporteren.[49] Empatica zet de E4 in de markt voor experimenteel onderzoek en pilots/ proeftuinen op een enkele locatie en de *Embrace2* voor grotere klinische studies

[48] www.empatica.com/embrace2

[49] https://support.empatica.com/hc/en-us/articles/203934665-Differences-between-Embrace-and-E4

met meer deelnemers op meerdere locaties. Anders dan bij de E4, verbinden de onderzoeksdeelnemers bij het gebruik van de *Embrace2,* de band via bluetooth met hun eigen mobiele apparaat en een eigen account, het is daardoor niet nodig om naar het lab te komen om de gegevens met de onderzoekers te delen. De bijbehorende app (*Mate App*), waarin de dragers hun eigen metingen kunnen zien, verzendt de verzamelde gegevens automatisch naar Empatica's cloud, waarna de onderzoeker de metingen terug kan zien in het *Research Portal* van Empatica (dit is niet hetzelfde portal als *E4 Connect*).

De *EmbracePlus*[50] is nog niet daadwerkelijk beschikbaar, maar kan al wel gereserveerd worden. Deze polsband, bedoeld voor grootschalig neurologisch onderzoek, meet dezelfde signalen als de E4 aangevuld met een gyroscoop en een stappenteller. Ook dit product zal gebruikmaken van een online omgeving.

Aangezien alle polsbanden van Empatica automatisch gebruikmaken van gegevensopslag in de cloud en niet (gemakkelijk) lokaal te gebruiken zijn, zullen ze grotendeels dezelfde voor- en nadelen hebben ten aanzien van dataveiligheid en privacy.

4.3 Wearables voor onderzoek of behandeling

Naast Empatica zijn er een aantal andere bedrijven die wearables voor klinisch onderzoek en behandeling aanbieden. Een aantal van deze producten beschrijven we in deze paragraaf. Hierbij richten we ons voornamelijk op producten die net als de Empatica E4 huidgeleiding kunnen meten. We bespreken hieronder eerst een aantal wearables die goed draagbaar zijn, vervolgens een aantal wearables die werken met plaksensoren (*Shimmer3* en *Move 4*) en daarna twee pakketten om zelf een wearable samen te stellen. Als laatste bespreken we nog een goed draagbare wearable die alleen hartslag (ecg) kan meten.

Het Zwitserse bedrijf Biovotion, recent overgenomen door het Amerikaanse Biofourmis, bood met de *Everion* een wearable aan die om de bovenarm gedragen wordt. Deze is beschikbaar in twee versies: een band gericht op gezondheid en fitness en een band specifiek bedoeld als medisch hulpmiddel. Laatstgenoemde band meet 22 verschillende medisch gevalideerde parameters, waaronder huidgeleiding, hartslag, bloeddruk, bloedzuurstofgehalte, huidtemperatuur, ademhalingsfrequentie en aspecten van slaapkwaliteit. Het bevat onder andere PPG- en EDA-sensoren. Deze band maakt net als de Empatica E4 gebruik van een app op mobiele apparaten met bluetoothverbinding, automatische uploads naar de cloud en een online dashboard waarin de onderzoekers de metingen kunnen inzien, beheren en downloaden. Na de overname van Biovotion door Biofourmis[51] is de band opgenomen in het *Biovitals*[52] ecosysteem, waar ook *Biovitals Research*[53] onderdeel van is. Dit platform biedt een aantal tools voor klinische onderzoeken die met behulp van de *Everion* uitgevoerd kunnen worden. Helaas is op de website van Biofourmis geen informatie te vinden over de beveiligings- en privacymaatregelen die getroffen zijn om de met de *Everion* verzamelde fysiologische gegevens te beschermen; deze informatie was op de web-

[50] www.empatica.com/embraceplus

[51] www.prnewswire.com/news-releases/biofourmis-announces-acquisition-of-biovotion-ag-completing-biovitals-platform-to-deliver-precise-interventions-at-the-right-time-to-manage-patients-with-complex-chronic-conditions-300959700.html

[52] www.biofourmis.com/biovitals

[53] www.biofourmis.com/solutions

site van Biovotion wel beschikbaar. Het is daardoor op dit moment onbekend hoe hiermee in de nieuwe situatie wordt omgegaan. Ook is onduidelijk wat de gevolgen van de overname zijn voor gebruikers die de *Everion* al voor die tijd hadden aangeschaft en wat er met de gegevens is gebeurd die toen al verzameld waren. Dit voorbeeld laat zien dat overnames door andere bedrijven invloed kunnen hebben op de continuïteit van een clouddienst en onzekerheid met zich mee kunnen brengen met betrekking tot de gegevens die daarin staan.

Het Fins bedrijf Vigofere Oy heeft een ring gericht op stressmanagement ontwikkeld genaamd *Moodmetric*.[54] Deze ring, die om de vinger wordt gedragen, meet huidgeleiding (EDA) en kan ook ingezet worden in veldonderzoek.[55] Voor gebruik binnen een onderzoekssetting zijn er verschillende mogelijkheden om toegang te krijgen tot de fysiologische gegevens.[56] Dit kan door gebruik te maken van de aangeboden clouddienst, door de aangeboden API te gebruiken, door zelf een app te ontwikkelen, of door de gegevens naar een Windows-computer te streamen via bluetooth (hiervoor is een dongel nodig). Het is niet mogelijk ruwe gegevens direct van het geheugen van de ring af te halen. De cloudoplossing is het eenvoudigst (en wordt door het bedrijf aanbevolen voor veldonderzoek). De gegevens worden bij het gebruik van deze oplossing automatisch geüpload naar de cloud. Vanuit de cloud is het mogelijk om de fysiologische gegevens te downloaden in verschillende formaten. Deze kunnen vervolgens met software naar keuze verder verwerkt worden. De ring biedt een aantal voordelen ten opzichte van de Empatica E4:

- het is altijd mogelijk de metingen (lokaal) te bekijken via de mobiele *Moodmetric* app, het is daarvoor niet verplicht om aan te melden voor de clouddienst;
- daarnaast is het mogelijk om de gegevens direct vanaf de ring te streamen via bluetooth naar een computer en op te slaan op een computer;
- volgens de privacyverklaring[57] worden de gegevens bij het gebruik van de clouddienst opgeslagen op servers in Finland (*Yoso Oy*) en nooit buiten de EU.

Het Amerikaanse bedrijf Equivital heeft ook een draagbare wearable voor onderzoek en monitoring op de markt gebracht genaamd *EQ02+ LifeMonitor*.[58] Deze borstband wordt aan een soort schouderriem gedragen en bevat sensoren om hartslag (ecg), ademhaling, huidtemperatuur en beweging (accelerometer) te meten. Daarnaast is het mogelijk extra sensoren toe te voegen, bijvoorbeeld om huidgeleiding (EDA-sensor), bloeddruk of zuurstofgehalte te meten.[59] De metingen kunnen ingezien worden door de sensormodule via bluetooth te verbinden aan een mobiel apparaat of computer. Equivital biedt verschillende softwareproducten aan om de metingen in realtime in te zien en/of te downloaden. Ook wordt een SDK aangeboden waarmee eigen applicaties ontwikkeld kunnen worden. Helaas biedt de website van het bedrijf relatief weinig informatie over het gebruik van het product en de bijbehorende software. Voor zover we kunnen beoordelen, is het mogelijk de metingen geheel lokaal in te zien.

[54] https://moodmetric.com

[55] https://moodmetric.com/services/research

[56] https://moodmetric.com/services/research/data-use-and-research-guides

[57] https://moodmetric.com/privacy-policy

[58] www.equivital.com/assets/common/EQ02+_08_Equivital_Data_Sheets_v8_(003).pdf

[59] www.equivital.com/products/tnr/TnR%20Accessories

Een ander bedrijf dat wearables voor onderzoeksdoeleinden aanbiedt is Shimmer.[60] Het biedt verschillende producten aan die verschillende fysiologische signalen meten. De *Shimmer3 GSR+*[61] biedt bijvoorbeeld, net als de Empatica E4, metingen van huidgeleiding (EDA), hartslag (PPG) en beweging. Dit product wordt ook om de pols gedragen, maar bevat wel verschillende draden naar sensoren die op andere plaatsen op het lichaam worden aangebracht (zoals de vingers). Daarnaast is er de *Shimmer3 ECG;*[62] een borstband met losse sensoren die onder andere op de borst worden geplakt. Dit instrument meet de hartslag (ecg) en bevat daarnaast een accelerometer en gyroscoop. Deze wearables zijn door het gebruik van plaksensoren vooral bedoeld voor gebruik in een lab met ondersteuning van een professional. De gegevens worden opgeslagen op een microSD-kaart in de *Shimmer3*. Om de gegevens te kunnen uitlezen op een computer, wordt gebruikgemaakt van een USB-verbinding (dit gaat via een dock of basisstation waarin de apparaatjes worden geplaatst) of een bluetooth-verbinding. Om de metingen te kunnen gebruiken kan software die door Shimmer beschikbaar wordt gesteld gebruikt worden, maar het is ook mogelijk om externe software zoals *MATLAB* te gebruiken of om eigen software te ontwikkelen. Ook is het mogelijk om de gegevens via bluetooth te streamen naar een mobiel (*Android*) apparaat. Deze producten hebben als voornaamste voordeel dat het mogelijk is de fysiologische gegevens volledig lokaal op te slaan en te beheren. De producten bieden daarnaast enorm veel configuratiemogelijkheden: de gebruiker kan bijvoorbeeld zelf bepalen welke sensoren aangesloten/gebruikt worden en zo alleen de metingen doen die nodig zijn voor het onderzoek (conform het principe van dataminimalisatie). Ook kan de gebruiker zelf kiezen hoe en wanneer de gegevens worden overgezet naar de computer. Dit gaat niet automatisch. Wel lijken de apparaten daardoor wat lastiger in gebruik dan de Empatica E4 of andere wearables. Een aandachtspunt is daarnaast dat de gemeten gegevens niet door Shimmer beschermd worden en ook niet geanonimiseerd zijn (zie ook paragraaf 1.3), hier moet de gebruiker zelf voor zorgen: '*It should be understood from the outset and you should communicate to test subjects that the physiological data that is streamed, stored, and analyzed through use of the device is not anonymized or privacy-protected in any way and you should take appropriate precautions in the protection and handling of such data in your research activities. Shimmer itself may buffer raw physiological data unencrypted on the integrated flash memory device. RF data streaming from the Shimmer may not be encrypted and could be intercepted by others.*' (www.shimmersensing.com/images/uploads/docs/Shimmer_User_Manual_rev3p.pdf, p. ii)

Ook het Duitse bedrijf Movisens[63] biedt verschillende mobiele sensoren voor onderzoeksdoeleinden aan, bijvoorbeeld de *EcgMove 4*[64] dat is gericht op het meten van ecg en fysieke activiteit. Dit is een klein apparaatje dat metingen kan doen door het met een band onder de borst te dragen of door het aan twee elektroden die onder de borst geplakt worden te bevestigen. Een ander product is de *EdaMove 4* dat huidgeleiding (EDA) en fysieke activiteit meet. Dit product wordt om de pols gedragen waarbij twee elektroden worden bevestigd aan de handpalm. Beide producten kunnen zowel offline als online gebruikt worden. Alleen in de online modus is het mogelijk om live metingen te zien (op een mobiel apparaat via bluetooth). In de

[60] www.shimmersensing.com

[61] www.shimmersensing.com/products/shimmer3-wireless-gsr-sensor

[62] www.shimmersensing.com/products/shimmer3-ecg-sensor

[63] www.movisens.com

[64] www.movisens.com/en/products/ecg-sensor

[64] www.movisens.com/en/products/eda-and-activity-sensor

offline modus worden de gemeten fysiologische gegevens uitgelezen door het apparaatje via USB te verbinden met de computer. Movisens biedt software aan om de sensor te configureren en uit te lezen. De ruwe gegevens worden dan lokaal opgeslagen en kunnen vervolgens geanalyseerd worden. Het bedrijf biedt aanvullende diensten en software aan voor dataverwerking en -analyse. De onderzoeker kan er echter ook voor kiezen hier geen gebruik van te maken en de ruwe data met andere software te analyseren (het ruwe dataformaat waarin de gegevens worden opgeslagen, is daartoe gedocumenteerd op de website van Movisens). De producten van Movisens hebben als voordeel dat het mogelijk is de gegevens volledig lokaal op te slaan. Ook moet de onderzoeker de sensor steeds configureren en de meting starten, daarbij kan ook aangeven worden hoe lang de meting moet duren. Zo heeft de onderzoeker controle over wat er wanneer gemeten wordt. Door het gebruik van elektroden die op het lichaam van de drager moeten worden geplakt, lijken deze sensoren wel wat omslachtiger in gebruik dan bijvoorbeeld de Empatica E4. Ook zijn deze daarom vooral geschikt voor studies in een lab of op een vaste locatie. Een ander aandachtspunt is dat niet is vermeld hoe de metingen die worden opgeslagen op het apparaat zijn beveiligd zolang ze niet naar de computer zijn overgezet.

Het Spaanse bedrijf Libelium, biedt met *MySignals*[65] een ontwikkelplatform aan waarmee het mogelijk is zelf een meetinstrument samen te stellen voor onderzoek. Hiervoor biedt het een groot scala aan sensoren aan, waaronder sensoren om huidgeleiding (EDA), hartslag (ecg), bloeddruk, bloedzuurstofgehalte en temperatuur te meten.[66] Het kan als kant-en-klare hardware (*MySignals SW*) of als zelfbouwpakket gebaseerd op Arduino[67] (*MySignals HW*) gekocht worden.[68] Het eerste is gemakkelijker in gebruik, het tweede biedt de mogelijkheid om eigen sensoren toe te voegen. *MySignals SW* bestaat uit een klein apparaatje waar de gewenste sensoren gemakkelijk ingeplugd kunnen worden. Op deze manier is de onderzoeker in staat om zelf te bepalen welke metingen hij of zij wil doen. Hoe de sensor op het lichaam aangebracht wordt is afhankelijk van het type: de EDA-sensor werkt met vingersensoren, de ecg met plaksensoren voor op de borst. Het apparaatje zelf kan niet gemakkelijk op het lichaam gedragen worden, het is daarmee geen 'echte' wearable, maar is door het kleine formaat wel handzaam en draagbaar. Het apparaatje heeft een scherm waarop de metingen direct uitgelezen kunnen worden. Ook is het mogelijk om de metingen via bluetooth naar een app op een mobiel apparaat te verzenden of via wifi direct van het apparaatje naar de *Libelium Cloud*. Het is mogelijk om het apparaatje te gebruiken zonder dat gegevens naar de cloud worden gestuurd: de metingen zijn dan af te lezen van het scherm van het apparaatje of via een app op een mobiel apparaat, maar zijn dan niet nader te analyseren. Als de cloud gebruikt wordt, is het wel mogelijk om met de Cloud API ruwe data naar een andere locatie over te zetten. Met de *MySignals HW* is het daarnaast mogelijk om de gegevens direct naar een eigen cloudserver te versturen, met de *SW* is dit niet mogelijk. Ten opzichte van de Empatica E4 biedt dit product een slechtere draagbaarheid, het lijkt daarom vooral geschikt voor kortdurend gebruik op een vaste locatie. Het biedt wel meer flexibiliteit en variatie met betrekking tot de gebruikte sensoren en is relatief eenvoudig te configureren. Daarnaast is aanmelden voor de cloudservice niet verplicht en kunnen de metingen eenvoudig afgelezen worden van het apparaat.

---

[65] www.my-signals.com

[66] www.libelium.com/downloads/documentation/mysignals_technical_guide.pdf

[67] www.arduino.cc

[68] www.my-signals.com/#platforms-mysignals

Een ander bedrijf dat pakketten aanbiedt waarmee zelf een eigen meetinstrument voor onderzoeksdoeleinden samengesteld kan worden, is het Portugese PLUX. Dit bedrijf biedt verschillende platformen aan: *BITalino*[69] en *biosignalsplux*.[70] *BITalino* biedt goedkopere zelfbouwpakketten en is vooral geschikt om kennis te maken met biofeedback en voor prototyping. *Biosignalsplux* is duurder en biedt min of meer kant-en-klare producten aan. Dit platform is beter geschikt voor geavanceerd onderzoek.[71] De binnen dit platform aangeboden wearables bevatten geen EDA-sensor, maar bijvoorbeeld wel ecg (deze *CardioBAN* bevat daarnaast een accelerometer). Het bedrijf biedt daarnaast *research kits* (die niet op het lichaam te dragen zijn) aan die meer sensoren kunnen bevatten. Het meest uitgebreid is de *biosignalsplux Professional*.[72] In dit apparaatje (een hub) kunnen naar keuze in totaal acht bedrade sensoren geplugd worden, waaronder EDA, ecg, eeg en EMG-sensoren, een thermometer, bloeddrukmeter en accelerometer. Deze hub is enigszins vergelijkbaar met de hierboven beschreven *MySignals SW*. De hub is eenvoudig te configureren en bedienen, verzamelt de metingen van de sensoren en verstuurt deze via bluetooth naar een computer. Het is daarnaast ook mogelijk om de gegevens via USB naar een computer over te zetten. De metingen worden dan eerst op het interne geheugen van de hub opgeslagen. Het is mogelijk om metingen vooraf in te plannen zodat ze beginnen en stoppen op een bepaalde tijd. Dit product biedt de onderzoeker dus veel flexibiliteit en controle over wat er wanneer verzameld wordt. Voor het uitlezen en analyseren van de gegevens wordt gebruikgemaakt van *OpenSignals*-software.[73] De hub kan hiermee volledig lokaal gebruikt worden; de uitgelezen gegevens worden dan (alleen) op de gebruikte computer opgeslagen. Vanuit deze software is het mogelijk de gegevens te exporteren in verschillende formaten zodat ze in andere software verder geanalyseerd kunnen worden. Met verschillende API's is het daarnaast mogelijk om de gegevens direct in externe software zoals MATLAB in te lezen, of een eigen mobiele app te ontwikkelen. Dit product is minder draagbaar dan de Empatica E4, door de losse sensoren vooral geschikt voor gebruik op een vaste locatie, maar biedt wel veel meer mogelijkheden en de gegevens worden lokaal opgeslagen. Een aandachtspunt is hierbij wel dat het onduidelijk is hoe de gegevens op de hub en in de software beveiligd zijn en of deze bijvoorbeeld versleuteld worden opgeslagen.

Een laatste product, dat weliswaar geen huidgeleiding meet, maar wel een ecg-sensor bevat, wordt gemaakt door Lief Therapeutics[74]. De *Lief* is gericht op het monitoren van stress en meet onder andere hartritme en ademhaling. Het bestaat uit een patch die met stickers onder de borst wordt geplakt. De patch geeft directe feedback aan de drager door te trillen zodra het hartritme onder een bepaalde drempel komt. De drager kan dan ademhalingsoefeningen doen en wordt daarbij geholpen door de trillingen te volgen. Ook dit product maakt net zoals de Empatica E4 gebruik van een app op mobiele apparaten met bluetooth-verbinding. Het overzetten van gegevens kan ook na het dragen, de metingen worden lokaal opgeslagen totdat ze gesynchroniseerd zijn met de app. Via wifi worden de gegevens naar het *LiefRx* cloudplatform gestuurd. Het is ook mogelijk om de app zonder internetconnectie te gebruiken, maar dan zijn de gegevens alleen op het mobiele apparaat in te zien. De

[69] https://bitalino.com

[70] https://biosignalsplux.com

[71] https://bitalino.com/en/intended-use/42-quick-compare

[72] https://biosignalsplux.com/products/kits/professional.html

[73] https://biosignalsplux.com/products/software/opensignals.html

[74] www.getlief.com

Lief is gericht op zowel consumenten als behandelaars, maar lijkt minder geschikt voor onderzoeksdoeleinden. Het is ons niet bekend of het mogelijk is ruwe metingen van de ecg-sensor uit het platform te halen voor nadere analyse. Een aandachtspunt daarnaast is dat in de privacyverklaring van Lief Therapeutics[75] staat dat de '*de-identified data*' met derden gedeeld kunnen worden, onder andere voor *profiling*.

4.4 Wearables voor consumenten

Naast wearables die vooral gericht zijn op gebruik door professionals in onderzoek en/of behandeling, zijn er vele producten op de consumentenmarkt beschikbaar die ook voor onderzoek, behandeling of toezicht ingezet zouden kunnen worden. Enkele voorbeelden zijn de activiteitentrackers van Fitbit en Garmin, of smartwatches zoals de *Apple Watch* of smartwatches draaiende op *Wear OS* (van Google). Deze producten bieden wel een afleesbaar scherm voor directe feedback aan de drager, maar doorgaans (veel) minder sensoren dan de producten gericht op professionals.

In deze paragraaf bespreken we verschillende smartwatches, vooral met het oog op dataveiligheid en privacy. We kijken daarbij met name naar de bijhorende apps. Hierin zitten de voornaamste beveiligings- en privacyrisico's, omdat door gebruik te maken van een app de drager de gegevens (mogelijk) met een externe partij deelt. Een activiteitentracker of smartwatch is doorgaans via bluetooth gekoppeld aan een smartphone en voor het uitlezen van fysiologische gegevens voor nadere analyse is een speciale app op nodig.[76] Apps zijn beschikbaar vanuit externe partijen (bijvoorbeeld de *Sense-It*-app, de *Google Fit*-app of de *Gezondheid*-app van Apple), maar kunnen ook zelf ontwikkeld worden (bijvoorbeeld met de Apple *ResearchKit* of *HealthKit*, of de *Google Fit SDK*). De apps van de grote fabrikanten maken doorgaans gebruik van de cloud, waarmee het mogelijk is de metingen ook op andere apparaten (online) in te zien.

Hieronder geven we eerst een kort overzicht van recente ontwikkelingen op de consumentenmarkt. Daarna bespreken we een aantal producten en apps in detail: eerst bekende smartwatches en apps van twee grote partijen (Google en Apple), vervolgens één smartwatch en één ander type instrument waarmee huidgeleiding gemeten kan worden.

De ontwikkelingen op de consumentenmarkt gaan razendsnel. In september 2020 bracht Fitbit bijvoorbeeld als eerste grote fabrikant een consumentenwearable met een EDA-app op de markt (de *Fitbit Sense*).[77] Apple bracht bijna gelijktijdig een nieuwe versie van de *Apple Watch* uit waarmee het zuurstofgehalte in het bloed gemeten kan worden. Ook Amazon werkt aan een polsband gericht op gezondheidsmetingen (de *Halo Band*),[78] die voorlopig alleen in de Verenigde Staten uitkomt. Dit product bevat niet alleen de bekende sensoren, maar doet ook op andere manieren metingen: met de camera van de smartphone kan het percentage lichaamsvet ge-

[75] www.getlief.com/privacy

[76] In sommige gevallen is het ook mogelijk om de gegevens op een computer uit te lezen. De *Fitbit* kan bijvoorbeeld met een Mac of Windows computer verbonden worden. Het is dan nog steeds nodig om een account aan te maken.

[77] https://tweakers.net/nieuws/171348/fitbit-introduceert-smartwatch-met-stresssensor.html

[78] https://tweakers.net/nieuws/171558/amazon-introduceert-halo-fitnessarmband-met-focus-op-gezondheidsmetingen.html en www.amazon.com/haloband

meten worden (de foto's zorgen voor een 3d-beeld van het lichaam dat door de software van Amazon geanalyseerd wordt). Stress kan volgens de fabrikant gemeten worden door het stemgeluid te laten analyseren via de microfoons van de smartphone (de software herkent stress in het stemgeluid).

Voor smartwatches met *Wear OS* zijn er verschillende apps beschikbaar om de fysiologische gegevens in te kunnen zien en op te slaan. Een bekend voorbeeld is *Google Fit.*[79] Zolang deze app niet geïnstalleerd is op de smartphone van de drager, worden er ook geen gegevens verzameld door Google. Bij installatie vraagt de app om rechten voor het gebruik van de gegevens van de verschillende sensoren (waaronder gps en PPG). In *Google Fit* worden daarna activiteitgegevens, locatiegegevens, lichaamssensorgegevens en gegevens over slaap opgeslagen. De opgeslagen gegevens worden bijgehouden in het gekoppelde Google-account en kunnen gedeeld worden met andere apps en apparaten. Via de instellingen kan de toegang tot de gegevens ingetrokken worden en kunnen de gegevens die al verzameld zijn, verwijderd worden.[80] Enkel het deinstalleren van de app of het uitloggen uit de app verwijdert de reeds opgeslagen gegevens niet, maar stopt wel het verzamelen van nieuwe gegevens. De gebruiker moet dus maar net weten dat het verwijderen van gegevens via de instellingen gaat en het deinstalleren van de app alleen niet voldoende is. Een nadeel van *Google Fit* is dat de privacyverklaring van Google[81] nogal lang is en niet specifiek ingaat op *Google Fit* of de verzamelde fysiologische gegevens. Het is daardoor niet uit te sluiten dat Google deze gegevens gebruikt om persoonlijke advertenties te tonen en deze gegevens combineert met gegevens van andere diensten van Google.

Een ander bekend voorbeeld van een smartwatch is de *Apple Watch*.[82] Versie 5 van deze smartwatch bevatte al verschillende sensoren waaronder een PPG- en ecg-hartslagsensor, gps, accelerometer en gyroscoop. De in september 2020 gelanceerde versie 6 bevat daarnaast een sensor waarmee het mogelijk is zuurstofsaturatie te meten. De Apple Watch is te gebruiken met *Google Fit*, maar de *Gezondheid*-app van Apple ligt meer voor de hand. Deze biedt nagenoeg dezelfde functionaliteit als de variant van Google. De privacyverklaring van Apple[83] bevat een aparte sectie over deze app. Hierin staat dat de drager zelf bepaalt welke informatie in de app wordt bewaard en wie toegang heeft tot de gegevens. Deze gegevens worden in de app versleuteld (mits de telefoon is vergrendeld met toegangscode, vingerafdruk of *Face ID*). Als in *watchOs* en *iOS* tweestapsverificatie is aangezet, dan wordt van de gezondheidsgegevens een back-up gemaakt die onleesbaar is voor Apple.

Om (medisch-)wetenschappelijk onderzoek eenvoudiger te maken heeft Apple de *ResearchKit*[84] beschikbaar gesteld. Dit is een opensource-framework voor het bouwen van apps. Deelnemers kunnen dan met hun *iPhone* of *Apple Watch* deelnemen. Onderdeel van de *ResearchKit* is dat de deelnemers bepalen met welke onderzoeken ze mee willen doen en altijd precies weten welke gegevens gedeeld worden. Apps die met dit framework ontwikkeld worden, moeten de deelnemers expliciet vragen om informed consent en toegang tot de benodigde gegevens.[85] Apps moeten altijd

[79] www.google.com/fit

[80] https://support.google.com/accounts/answer/6098255

[81] https://policies.google.com/privacy?hl=nl

[82] www.apple.com/nl/watch

[83] www.apple.com/nl/privacy/features

[84] www.apple.com/nl/researchkit en http://researchkit.org

[85] http://researchkit.org/hig

eerst toestemming van de deelnemers vragen en deelnemers informeren over het recht op vertrouwelijkheid en de manier waarop gegevens worden behandeld en gedeeld. Deze apps moeten bovendien door een onafhankelijke ethische commissie zijn goedgekeurd voordat de studie van start kan gaan. Geïntegreerd met *HealthKit* kunnen ook gezondheidsgegevens meegenomen worden in de studie. Alle apps in de *App Store* moeten hun privacybeleid verplicht openbaar maken. Dit geldt ook voor alle apps die met *HealthKit* werken. De gegevens gebruiken voor advertentie- of dataminingdoeleinden is niet toegestaan. Het delen van de gegevens met de app gaat rechtstreeks van *HealthKit* naar die app en loopt niet via het netwerk van Apple. Aandachtspunt hierbij is dat in de privacyverklaring staat: 'bij sommige onderzoeken met ResearchKit wordt Apple mogelijk vermeld als onderzoeker, zodat we gegevens ontvangen van deelnemers die daar toestemming voor geven. Aan de hand van die informatie kunnen we nagaan hoe onze technologie kan bijdragen aan de manier waarop mensen hun gezondheid in de gaten houden. Bij het verzamelen van deze gegevens worden de deelnemers niet direct aan Apple bekendgemaakt.'

Recentelijk bracht Fitbit een smartwatch uit waarmee ook huidgeleiding gemeten kan worden: de *Fitbit Sense.*[86] Deze wearable bevat daarnaast onder andere een ecg-sensor, een huidthermometer, een accelerometer en gyroscoop. Om huidgeleiding te kunnen meten moet de gebruiker de *EDA Scan*-app gebruiken en de handpalm boven het apparaat houden. Het meet dit dus niet direct van de pols. De *Sense* kan gebruikt worden met Fitbits eigen app[87], maar ook met apps van andere partijen. Voor het gebruik van de Fitbit-app moet een account bij Fitbit aangemaakt worden. Hiervoor dient de gebruiker onder andere de volgende persoonsgegevens te delen: naam, geboortedatum, gewicht en lengte. In de privacyverklaring[88] benoemt Fitbit expliciet dat de fysiologische gegevens verzameld worden. Zodra de smartwatch synchroniseert met de app, worden de gegevens naar de servers van Fitbit overgezet. Het is mogelijk om gesynchroniseerde gegevens (of een deel daarvan) achteraf te verwijderen. Ook als het hele account verwijderd wordt, worden de fysiologische gegevens verwijderd. De gegevens kunnen dan echter al met derden gedeeld zijn. '*These partners provide us with services globally, including for customer support, information technology, payments, sales, marketing, data analysis, research, and surveys*'.

Naast deze smartwatches, hebben we op de consumentenmarkt één ander product gevonden dat naast hartslag ook huidgeleiding kan meten, eveneens met een polsband. Dit is de *GoBe2*[89] van het Amerikaanse bedrijf HEALBE. Dit product gericht op toepassingen op het gebied van gewichtsverlies en gezondheid, kan gebruikt worden om calorie-inname, hydratatie, slaap, stress en activiteit bij te houden. Het bevat een EDA-sensor op basis waarvan de gebruiker een waarschuwing krijgt als de emotionele spanning langer duurt dan 10 minuten. Deze polsband bevat een simpel scherm waarop de gebruiker de laatste metingen of waarschuwingen kan zien. Daarnaast zijn de metingen terug te zien via een app op een mobiel apparaat (verbonden via bluetooth). Deze metingen worden automatisch in de cloud opgeslagen. Via het online dashboard is het mogelijk de band te integreren met andere platformen zoals *Apple Health* of *Google Fit*. De fysiologische gegevens van de drager worden automatisch door Healbe verzameld. Deze gegevens worden in sommige

[86] www.fitbit.com/nl/sense

[87] www.fitbit.com/nl/app

[88] www.fitbit.com/nl/legal/privacy-policy

[89] https://healbe.com/eu

gevallen gedeeld met andere partijen: '*Healbe may also share your personal information with companies who provide services such as information processing, analytics, order fulfillment, product delivery, customer data management, customer research and the like. These companies are obligated to protect your information and may be located wherever Healbe does business.*'[90]

4.5 Samenvatting en discussie

In dit hoofdstuk hebben we twee soorten wearables beschreven: wearables die primair gericht zijn onderzoek en behandeling begeleid door professionals en wearables die vooral bedoeld zijn voor gebruik door consumenten in het dagelijks leven. De belangrijkste eigenschappen van deze wearables worden samengevat in tabel 1. De wearables zijn hierin geordend in de volgorde waarin ze in de voorgaande paragrafen beschreven zijn.

[90] https://healbe.com/eu/privacy/

Tabel 1 Overzicht van de bekeken wearables

Naam	Doelgroep	Doeleinde	Sensoren	Toepassing	Directe feedback mogelijk	Locatie gegevens	Transport gegevens
Empatica E4	Professional	Onderzoek	EDA, PPG, accelerometer, huidthermometer	Polsband	Via app op mobiel apparaat	Cloud	Bluetooth of USB, en internet
Embrace2	Consument en professional	Zorg en onderzoek	EDA, accelerometer, gyroscoop, huidthermometer	Polsband	Via app op mobiel apparaat	Cloud	Bluetooth en internet
EmbracePlus	Professional	Onderzoek	EDA, PPG, accelerometer, gyroscoop, huidthermometer	Polsband	n.n.b[a]	n.n.b[a]	n.n.b[a]
Everion	Consument en professional	Zorg en onderzoek	o.a. EDA, PPG, accelerometer, huidthermometer, pulsoxymeter	Band om bovenarm	Via app op mobiel apparaat	Cloud	Bluetooth en internet
Moodmetric	Consument en professional	Zorg en onderzoek	EDA	Ring om vinger	Via app op mobiel apparaat	Lokaal of cloud	Bluetooth (en internet)
EQ02+	Professional	Zorg en onderzoek	ecg, accelerometer, huidthermometer, o.a. EDA (extern)	Borstband met schouderriem	Via app op mobiel apparaat	Lokaal	Bluetooth
Shimmer3 GSR+ en *ECG*	Professional	Onderzoek	o.a. EDA en PPG, of ecg, accelerometer, gyroscoop	Polsband plus sensoren op o.a. vingers resp. borstband plus plaksensoren op o.a. borst	Via app op mobiel apparaat	Lokaal	Bluetooth of USB
EdaMove 4 en *EcgMove 4*	Professional	Onderzoek	o.a. EDA of ecg, accelerometer, gyroscoop, huidthermometer	Polsband plus plaksensoren op handpalm resp. borstband of plaksensoren op borst	Via app op mobiel apparaat	Lokaal	Bluetooth of USB
MySignals SW	Professional	Onderzoek	o.a. EDA, ecg, huidthermometer, pulsoxymeter	Apparaatje met bedrade sensoren	Via scherm op apparaatje, app op mobiel apparaat of software op computer	Lokaal (beperkte functionaliteit) of cloud	Bluetooth (en internet)
Biosignalsplux	Professional	Onderzoek	o.a. EDA, ecg, accelerometer, huidthermometer	Apparaatje met bedrade sensoren	Via software op computer	Lokaal	Bluetooth of USB
Lief	Consument en professional	Zorg	ECG	Patch op borst	Via trillingen van de patch en app op mobiel apparaat	Cloud	Bluetooth en internet
Wear OS met Google Fit	Consument	Dagelijks gebruik	Afhankelijk van device, doorgaans PPG, accelerometer, gyroscoop, GPS	Polsband	Via scherm op polsband en app op mobiel apparaat	Cloud	Bluetooth, internet
Apple Watch	Consument	Dagelijks gebruik	PPG, ecg, accelerometer, gyroscoop, GPS, pulsoxymeter (versie 6)	Polsband	Via scherm op polsband en app op mobiel apparaat	Cloud	Bluetooth, internet
Fitbit Sense	Consument	Dagelijks gebruik	o.a. EDA, ecg, huidthermometer, accelerometer, gyroscoop, GPS, pulsoxymeter	Polsband	Via scherm op polsband en app op mobiel apparaat	Cloud	Bluetooth, internet
GoBe2	Consument	Gezondheid	EDA, PPG, accelerometer	Polsband	Via scherm op polsband en app op mobiel apparaat	Cloud	Bluetooth, internet

[a] Deze wearable is nog niet op de markt, daarom zijn een aantal aspecten nog niet bekend.

Wat opvalt als gekeken wordt naar instrumenten die bedoeld zijn voor onderzoek en behandeling is dat er grofweg twee varianten zijn: 1) wearables of draagbare apparaatjes voor gebruik in een lab of op een vaste locatie; en 2) wearables geschikt voor onderzoek op grotere schaal en/of behandeling op afstand, met veel verschillende deelnemers op verschillende locaties. Voor de eerste groep zijn er offline-oplossingen beschikbaar. Deze wearables bieden ook meer configuratiemogelijkheden voor de onderzoekers en behandelaars, waarbij deze zelf kunnen bepalen welke metingen worden verzameld en waar deze worden opgeslagen. De onderzoeker of behandelaar is er dan ook zelf verantwoordelijk voor maatregelen te nemen om de gegevens te beveiligen. Door de vele mogelijkheden lijken sommige van deze wearables wel meer technische expertise te vergen voor het gebruik. Bij de tweede groep wearables valt op dat alle aanbieders voor een cloudoplossing kiezen. Hierdoor is het voor onderzoekers en behandelaars gemakkelijker om grotere studies uit te voeren of grotere groepen op afstand te behandelen. Daarnaast is het deelnemen aan een studie of behandeling voor de dragers laagdrempeliger: het is niet nodig om naar een lab of zorglocatie te komen, de band kan langdurig thuis gedragen worden (sommige producten zijn zelfs waterdicht) en het kost weinig moeite om de metingen naar de onderzoeker of behandelaar te sturen omdat dit grotendeels geautomatiseerd is. Bij sommige producten kunnen de dragers ook inzicht krijgen in hun eigen metingen door gebruik te maken van een mobiele app (geen van de producten heeft een scherm dat direct afleesbaar is). Doordat de gegevens altijd en vaak automatisch naar de cloud worden gestuurd, is het van groot belang en volgens de privacywetgeving zelfs verplicht om door een (privacy) jurist een goede verwerkersovereenkomst met de fabrikant te laten afsluiten, en onder andere af te spreken in welk land de gegevens worden opgeslagen, wie er toegang tot de gegevens krijgt en hoe lang deze bewaard worden. Waar van toepassing, is in dit onderzoek gekeken naar de privacyverklaring van de fabrikanten, zodat we een beeld krijgen van hoe er 'standaard' met de verzamelde (fysiologische) gegevens wordt omgegaan. Het lag buiten de scope van dit onderzoek om bij alle partijen na te gaan of het mogelijk is een verwerkersovereenkomst met specifieke voorwaarden af te sluiten die aan de geldende privacywetgeving voldoet.

Het gebruik van reguliere (consumenten) smartwatches voor onderzoek, behandeling of toezicht is ook mogelijk. Dit heeft als voordeel dat de drager zelf de metingen in de gaten kan houden (door gebruik van het direct afleesbare scherm en/of gebruik van een app) en tegelijkertijd ook de andere functionaliteiten van de smartwatch kan gebruiken. Als steeds meer mensen een smartwatch voor persoonlijk gebruik hebben, zal het deelnemen aan onderzoek, behandeling of toezicht waarschijnlijk laagdrempeliger worden en kan zo het aantal deelnemers groter worden. Een nadeel voor dit gebruik is dat deze instrumenten op dit moment nog (veel) minder sensoren hebben dan de producten gericht op professionals. Er zijn bijvoorbeeld nog niet veel smartwatches die een EDA-sensor bevatten, maar veel smartwatches bevatten wel een PPG- of ecg-sensor. Ook zijn de sensoren mogelijk niet altijd gevalideerd (Cosoli et al., 2020; Shcherbina et al., 2017). Voor het uitlezen van fysiologische gegevens voor nadere analyse is daarnaast een app op een mobiel apparaat nodig. Een smartwatch slaat namelijk meestal zelf geen gegevens op en heeft lang niet altijd een wifiverbinding, maar is doorgaans wel via bluetooth gekoppeld aan een smartphone. De gegevens worden nadat ze via bluetooth naar de smartphone zijn verzonden, lokaal opgeslagen op de smartphone en/of opgeslagen in de cloud, afhankelijk van de gekozen app. Voordat smartwatches worden ingezet in wetenschappelijk onderzoek of voor behandeling of toezicht is het van belang om met de aanbieder van de app die wordt gebruikt voor het uitwisselen of uitlezen van gegevens een goede verwerkersovereenkomst af te sluiten en/of na te gaan of de

geboden standaardvoorwaarden voldoen aan de op het gebruik van toepassing zijnde privacywetgeving.

Een belangrijke kanttekening bij het gebruik van consumentenwearables is dat uit onderzoek van het FD blijkt dat fabrikanten zich doorgaans niet aan de geldende privacywetgeving houden.[91] Volgens het FD stellen acht bekende fabrikanten desgevraagd zich aan de Europese privacyregels te houden: Apple, Fitbit, Xiaomi, Huawei, Withings (Nokia), Samsung, Polar en Garmin. Tegelijkertijd delen bijna alle fabrikanten de verzamelde fysiologische gegevens met derden, zijn ze onduidelijk over het doel van de gegevensverzameling, en sturen ze de gegevens naar landen buiten de EU (vooral naar de Verenigde Staten). Het FD constateert dat veel privacyverklaringen onduidelijk of incompleet zijn. Dat is ook onze bevinding. Daar komt bij dat deze verklaringen veelal zijn gericht op gebruikers die ook zelf drager van de wearable zijn. Het is (behalve voor Apple's *Research Kit*) onbekend hoe deze aanbieders omgaan met gebruik voor andere doeleinden zoals wetenschappelijk onderzoek, behandeling of toezicht. Het is dan ook de vraag of het mogelijk is om als niet-dragende gebruiker (individu of instituut) een verwerkersovereenkomst met deze partijen af te sluiten die voldoet aan de geldende privacywetgeving. In het advies van ICTRecht (2019) met betrekking tot de opslag van medische gegevens in de cloud wordt ook gewaarschuwd dat verschillende cloudproviders in hun voorwaarden naar hun eigen verwerkersovereenkomst verwijzen en ieder ander model van de hand wijzen.

4.6 Vergelijking met de Empatica E4 wat betreft dataveiligheid, privacy en geboden functionaliteit

De E4 van Empatica heeft als belangrijkste voordeel dat zowel hartslag (PPG) als huidgeleiding (EDA) kunnen worden gemeten met één makkelijk toepasbaar instrument. De belangrijkste nadelen met betrekking tot dataveiligheid en privacy zijn dat lokaal gebruik niet tot de standaardmogelijkheden behoort en dat de cloudomgeving beter beveiligd kan worden. Door het gebruik van een cloud is het daarnaast nodig om een verwerkersovereenkomst met Empatica af te sluiten om aan de privacywetgeving te voldoen. In deze paragraaf beschouwen we of er wearables zijn die dezelfde voordelen bieden, maar beter presteren op het gebied van dataveiligheid en privacy.

De *EcgMove 4*, *EdaMove 4*, *Moodmetric*, *EQ02+, Shimmer3 GSR+*, *Shimmer3 ECG, MySignals SW en biosignalsplux* kunnen volledig lokaal gebruikt worden, zonder dat gebruik hoeft te worden gemaakt van de cloud. Belangrijke beveiligings- en privacygerelateerde nadelen (van de Empatica E4) gelden dan niet: het risico dat gegevens onderschept of gestolen worden is kleiner, en de gebruiker heeft dan niet te maken met een externe partij waar de gegevens worden opgeslagen, en behoudt zelf de controle over wat er met de gegevens gebeurt. In dit geval is er ook geen externe verwerker, en een verwerkersovereenkomst afsluiten is niet nodig. De *EcgMove 4* en *Moodmetric* zijn net als de Empatica E4 eenvoudig toepasbaar doordat zij bestaan uit een borstband of ring om de vinger. De andere instrumenten zijn lastiger te gebruiken, omdat er naast een polsband, borstband, of hub ook losse (plak)sensoren nodig zijn. Wat meetopties betreft zijn de *MySignals SW*- en *biosignalsplux*-apparaatjes het meest uitgebreid. Hierop kunnen naar behoefte tot wel acht verschillen-

[91] https://fd.nl/futures/1355712/fabrikanten-slimme-horloges-voldoen-niet-aan-europese-privacynorm en https://fd.nl/futures/1356905/zelfs-datanerd-gaat-niet-met-slim-horloge-naar-bed

de sensoren aangebracht worden waaronder eeg, EMG, EDA en ecg. Dit zijn echter geen echte wearables, maar eerder compacte apparaatjes. Van de meer draagbare wearables zijn de *EcgMove 4* en *EdaMove 4* of de *Shimmer3 GSR+* en *Shimmer3 ECG* het meest compleet als ze in combinatie met elkaar gebruikt worden. Naast respectievelijk ecg- en EDA-sensoren omvatten deze instrumenten ook een accelerometer en gyroscoop. De *Move 4*-producten bevatten daarnaast ook nog een huidthermometer. Anders dan met de Empatica E4 is het voor beide combinaties echter wel nodig om met minder gebruiksvriendelijke plaksensoren te werken.

Van de producten die gebruikmaken van cloudopslag, komt de *Apple Watch* met enkele beveiligingsmaatregelen die Empatica niet aanbiedt, waaronder versleuteling van de gegevens op het mobiele apparaat en twee-factor-authenticatie om toegang te krijgen tot de cloud. De *Apple Watch* is daarnaast makkelijk toepasbaar en biedt de mogelijkheid tot realtime feedback via het scherm. De *Apple Watch* meet echter geen huidgeleiding, maar bevat wel een ecg-sensor en heeft daarnaast een PPG-sensor, accelerometer en gyroscoop.

Naast de Empatica E4 zijn er niet veel wearables op de markt die dezelfde combinatie van sensoren bieden en daarnaast gemakkelijk bruikbaar zijn. Alleen de *Everion* en de *Fitbit Sense* zijn wat dat betreft vergelijkbaar met de Empatica E4 (al meet de *Fitbit* huidgeleiding niet continu). Beide producten hebben echter ook nadelen ten opzichte van de Empatica E4 (die al langere tijd beschikbaar is bij een bedrijf met een goede reputatie): het zijn producten of aanbieders die nieuw op de markt zijn,[92] waardoor het onduidelijk is hoe toekomstbestendig ze zijn. De *Shimmer3 GSR+* bevat nagenoeg dezelfde sensoren als de Empatica E4 (waaronder EDA en PPG), maar maakt daarbij gebruik van (minder gebruiksvriendelijke) plaksensoren. De *EcgMove 4* is redelijk goed draagbaar, maar meet alleen in combinatie met de *EdaMove 4* huidgeleiding. Dit laatste product werkt dan wel weer in combinatie met plaksensoren. We hebben overigens niet onderzocht in hoeverre de genoemde wearables beter of slechter presteren wat betreft de validiteit, accuratesse en betrouwbaarheid van de metingen.

Meerdere instrumenten scoren echter beter dan de Empatica E4 wat betreft: 1) de mogelijkheid om het instrument volledig lokaal te gebruiken zonder dat de cloud nodig is; of 2) het bieden van een clouddienst met betere beveiligingsmaatregelen. Een voordeel van de Empatica E4 is echter wel dat Empatica gebruikt maakt van een custom binair formaat voor de opslag van gegevens in de cloud, een beveiligingsmaatregel die niet alle andere cloud-gebaseerde wearables bieden.

Deze beknopte vergelijking laat zien dat er verschillende wearables verkrijgbaar zijn die zouden kunnen voldoen voor gebruik in de justitiële context, afhankelijk van de benodigde sensoren en draagbaarheid, maar daarnaast ook voldoende waarborgen bieden wat betreft privacy en dataveiligheid (of dit doen na enige aanpassing). Wat dit betekent voor het gebruik van wearables in de justitiële context bespreken we in hoofdstuk 6.

[92] De *Everion* zelf is niet nieuw, maar de fabrikant is recentelijk overgenomen door een derde partij en wordt op een andere manier in de markt gezet.

5 Ervaringen van gebruikers

5.1 Inleiding

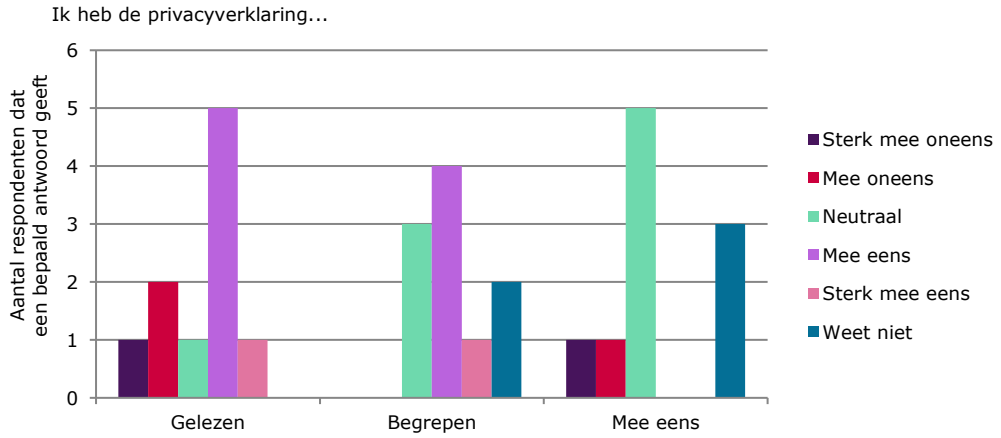
De Empatica E4 wordt door een (klein) aantal onderzoekers in Nederland gebruikt om fysiologische gegevens te verzamelen. Om de kennis en ervaringen van de gebruikers met betrekking tot de opslag van gegevens en toegang tot gegevens door derden bij de Empatica E4 te verkennen is een korte vragenlijst afgenomen (zie bijlage 2). Tien gebruikers van de Empatica E4 hebben de vragenlijst ingevuld. Dit zijn nagenoeg alle bij ons bekende gebruikers van de Empatica E4 in Nederland. Zij zijn benaderd op een bijeenkomst van het netwerk Wearables in Practice (6 april 2018). De gebruikers zijn voornamelijk onderzoekers en beleidsfunctionarissen bij universiteiten, zorginstellingen of justitiële instellingen.

In dit hoofdstuk bespreken we achtereenvolgens de ervaringen van de gebruikers met betrekking tot de privacyverklaring (paragraaf 5.2), de opslag van gegevens (paragraaf 5.3), de toegang tot gegevens door derden (paragraaf 5.4) en de kwaliteit van de verzamelde gegevens (paragraaf 5.5). We sluiten dit hoofdstuk af met een korte samenvatting in paragraaf 5.6.

5.2 Kennis van de privacyverklaring

Een kleine meerderheid van de gebruikers geeft aan de privacyverklaring te hebben gelezen (zie figuur 15).[93] De meesten van hen geven ook aan deze te begrijpen. De meerderheid van de gebruikers heeft een neutrale houding ten opzichte van de inhoud van de privacyverklaring, een derde weet niet of ze het ermee eens zijn. Enkele gebruikers zijn het oneens met de privacyverklaring.

Figuur 15 Kennis van de privacyverklaring van Empatica E4



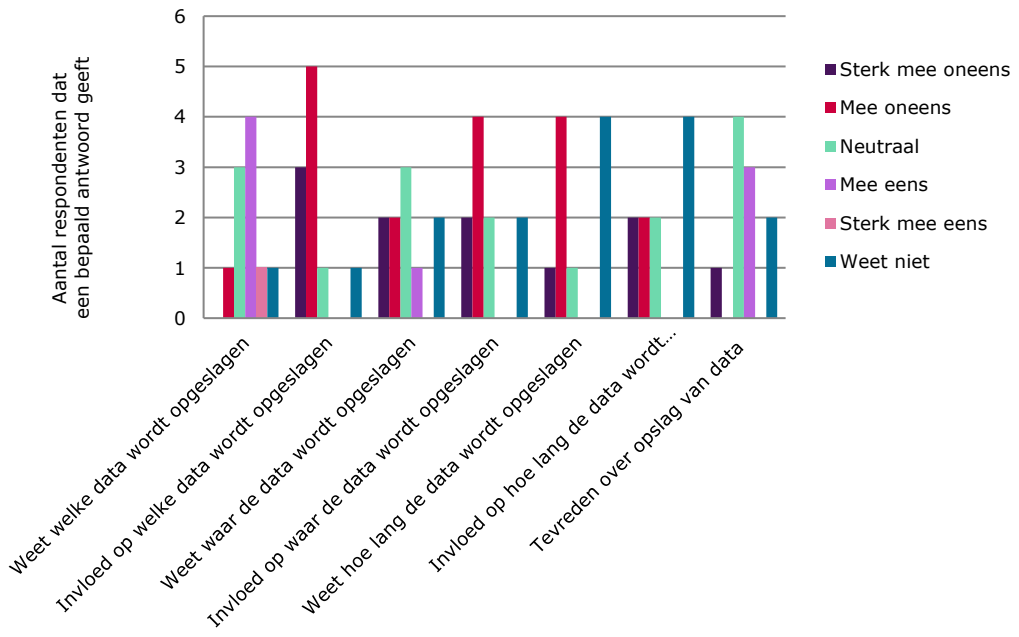
[93] De privacyverklaring is herzien na het afnemen van de vragenlijst n.a.v. de AVG. Deze is vooral explicieter ten opzichte van nieuwe regels in de AVG geworden. De vernieuwde verklaring gaat echter alleen over de persoonsgegevens van de gebruiker en niet over de verzamelde fysiologische gegevens en schept daarom geen helderheid over de opslag daarvan en de toegang daartoe.

5.3 Kennis over de opslag van de met Empatica E4 verzamelde gegevens

De meeste gebruikers geven aan te weten welke van de met de Empatica E4 verzamelde (fysiologische) gegevens opgeslagen worden door de fabrikant (zie figuur 16). Slechts een klein deel weet waar de fysiologische gegevens opgeslagen worden en geen van de gebruikers weet hoe lang de fysiologische gegevens opgeslagen worden.

De gebruikers geven aan geen invloed te hebben op welke gegevens worden opgeslagen, op de plaats waar deze worden opgeslagen of op hoe lang de gegevens worden opgeslagen. Niettemin is ongeveer een derde van de gebruikers tevreden over de gegevensopslag door Empatica. Het grootste deel van de gebruikers beantwoordt deze tevredenheidsvraag echter met 'neutraal' of 'weet niet'. Een enkeling is zeer ontevreden.

Figuur 16 Kennis over gegevensopslag door fabrikant Empatica



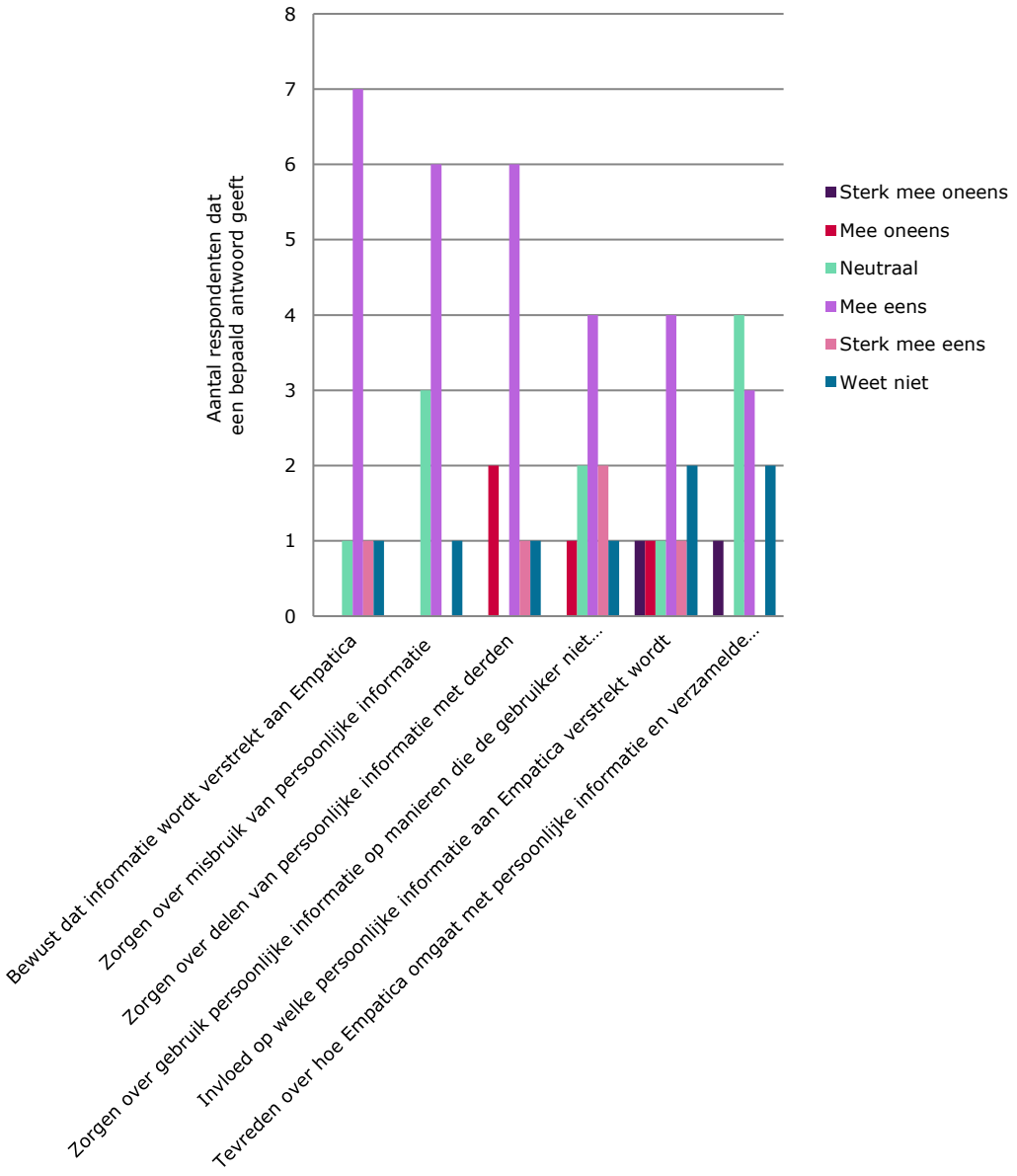
5.4 Toegang van derden tot de door Empatica verzamelde gegevens

Over het algemeen zijn gebruikers zich ervan bewust dat zij door de Empatica E4 te gebruiken persoonlijke informatie verstrekken aan de fabrikant Empatica (zoals naam en adresgegevens). Ongeveer twee derde van de bevraagde gebruikers maakt zich zorgen over eventueel misbruik van de door Empatica verzamelde gegevens (de persoonlijke gegevens van de gebruiker en/of de fysiologische gegevens van de drager), het delen van gegevens met derden, of over de mogelijkheid dat gegevens worden gebruikt op een manier die men niet voorzien heeft (zie figuur 17).

Circa de helft van de gebruikers ervaart dat hij of zij invloed heeft op welke informatie wordt verstrekt aan Empatica. Ondanks bovengenoemde zorgen, is een derde van de bevraagde gebruikers tevreden over hoe Empatica omgaat met persoonlijke

informatie en de verzamelde fysiologische gegevens, drie kwart is daarover neutraal of weet het niet en één gebruiker is daarover zeer ontevreden.

Figuur 17 Tevredenheid en zorgen over hoe Empatica omgaat met de door middel van de Empatica E4 verzamelde gegevens

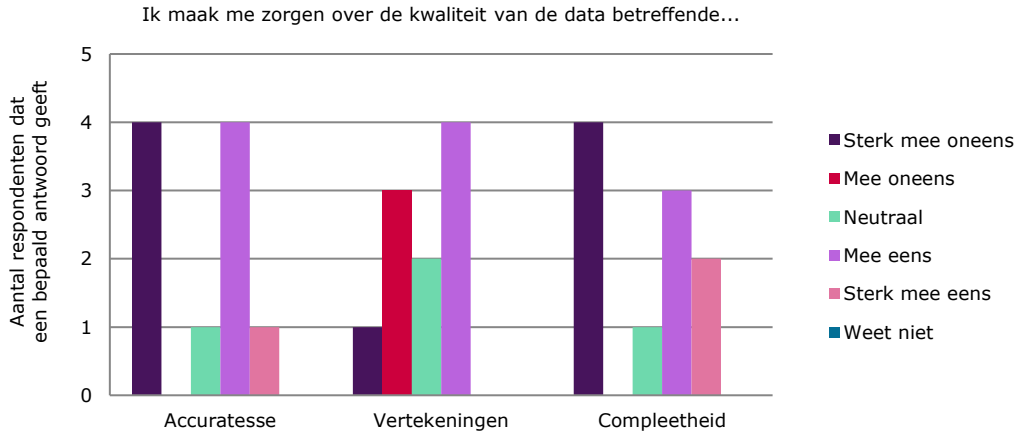


5.5 Kwaliteit van de gegevens verzameld met de Empatica E4

De ervaringen van de professionele gebruikers van de Empatica E4 ten aanzien van de kwaliteit van de verzamelde fysiologische gegevens lopen uiteen (zie figuur 18). Ongeveer de helft van hen maakt zich zorgen dat de verzamelde gegevens mogelijk incompleet of vertekend zijn, een deel maakt zich hier geen zorgen om en een enkeling is neutraal. In paragraaf 2.4 hebben we eerder al samengevat wat uit

wetenschappelijk onderzoek bekend is over de accuratesse en betrouwbaarheid van verzameling van gegevens met behulp van de Empatica E4.

Figuur 18 Zorgen over de kwaliteit van de met Empatica E4 verzamelde gegevens



5.6 Samenvatting en discussie

Hoewel een meerderheid van de gebruikers vooraf de privacyverklaring heeft doorgenomen, heeft ook een derde van de gebruikers dat niet gedaan. Het is daardoor ook niet verwonderlijk dat bij veel van de vragen men neutraal antwoordt of niet weet hoe Empatica omgaat met gegevensopslag en -toegang. Bijna geen enkele gebruiker weet waar en hoe lang de verzamelde gegevens worden opgeslagen. Ook maakt men zich zorgen over toegang door derden en misbruik van gegevens. Gebruikers maken zich dus zorgen over de veiligheid van gegevensopslag en -toegang, maar gebruiken niettemin de Empatica E4. Mogelijk gaat voor de in dit onderzoek bevraagde professionele gebruikers de 'privacy paradox' op. Een mogelijke verklaring voor het toch gebruiken van de Empatica E4 is dat er geen bruikbare of betaalbare alternatieven bekend waren bij de gebruikers. Een andere mogelijkheid zou kunnen zijn dat gebruikers erop vertrouwen dat alles goed geregeld is, mede door de goede reputatie die de ontwikkelaar van de Empatica E4, Rosalind Picard, heeft in het onderzoeksveld.

6 Discussie

6.1 Inleiding

In dit hoofdstuk komt aan de orde wat de bevindingen van ons casusonderzoek betekenen voor het gebruik van de Empatica E4 en vergelijkbare fysiologische wearables in de justitiële context. In paragraaf 6.2 beschrijven we de belangrijkste risico's van de Empatica E4 bij gebruik in een justitiële setting. Hierbij bespreken we eerst de veiligheidsrisico's en vervolgens de privacyrisico's. In paragraaf 6.3 gaan we in op de opties voor gebruik van een wearable in de justitiële context die volgen uit ons casusonderzoek. In paragraaf 6.4 ten slotte, formuleren wij conclusies en aanbevelingen.

6.2 Risico's van gebruik van de Empatica E4 in een justitiële context

6.2.1 Veiligheidsrisico's

Het is niet mogelijk de Empatica E4 alleen lokaal te gebruiken, tenzij er een app ontwikkeld wordt. Dit vergt echter veel technische knowhow en het is omslachtiger om de metingen op een computer te krijgen voor nadere analyse. Voor de meeste toepassingen ligt het daarom voor de hand gebruik te maken van de cloudomgeving die Empatica biedt (*E4 Connect*). Empatica heeft verschillende aspecten op het gebied van dataveiligheid van de cloud op orde, zoals opslag in een custom binair formaat bij een ISO-gecertificeerde host en versleuteling van de up- en download-verbindingen. Empatica stelt echter geen eisen aan het wachtwoord van de gebruiker voor de cloudomgeving en daarbij vindt geen twee-factor-authenticatie plaats. Hier ligt dus een grote verantwoordelijk bij de gebruikers om een veilig wachtwoord te kiezen, dat niet ook voor andere accounts of websites gebruikt wordt, en dit wachtwoord regelmatig te wijzigen. Door het ontbreken van eisen aan het wachtwoord en van twee-factor-authenticatie zou een account relatief gemakkelijk gehackt kunnen worden om de in het account verzamelde gegevens vervolgens te stelen. Ook is het niet uit te sluiten dat eventueel door onderschepping van het transport buitgemaakte (versleutelde) bestanden in het custom binair formaat door hackers met de juiste kennis ontsleuteld kunnen worden. Onbekend is verder hoe Empatica de API (benodigd om de bestanden in het custom binair formaat te lezen) beveiligd heeft tegen hacken en misbruik. Dit maakt het risico op het kunnen inzien van onversleutelde gegevens potentieel groter. Met toegang tot de API is het namelijk eenvoudiger om onderschepte gegevens leesbaar te maken.

Opslag in de (online) cloud brengt een groter risico met zich mee voor het digitaal onderscheppen of stelen van gegevens dan lokale (offline) opslag. In het geval van lokale opslag is dit moeilijker doordat er eerst fysieke toegang verkregen moet worden tot de opslag (terwijl de cloudopslag van afstand gehackt of aangevallen kan worden). Het risico op gegevensinbreuken wordt verder verkleind als de metingen op de wearable zelf worden versleuteld en als deze gegevens na overzetten op een computer worden geanonimiseerd. Bij lokaal gebruik is er daarnaast voor de gebruiker meer flexibiliteit en controle over bijvoorbeeld waar de verzamelde gegevens opgeslagen worden, en gegevens van dragers worden dan niet (automatisch) met een externe partij gedeeld. De gebruiker is dan wel zelf verantwoordelijk voor afdoende beveiliging van de apparaten waarop de gegevens worden opgeslagen en

geanalyseerd. De gebruiker zou in dat kader onder andere moeten voorzien in een informatiebeveiligingsbeleid en een beheerplan voor gebruik, opslag en management van de verzamelde gegevens. Als het gaat om informatiebeveiliging wordt vaak gebruikgemaakt van de BIV-classificatie waarbij de beschikbaarheid, integriteit en vertrouwelijkheid van gegevens wordt aangegeven.[94]

Het is moeilijk in te schatten wat de precieze risico's voor gebruik van de Empatica E4 in de justitiële context zijn. Er is een risico met betrekking tot de veiligheid van de gegevens maar hoe groot dit risico precies is, is lastig in te schatten. De aard van de gevaren is duidelijk, maar de grootte van de kans waarmee die zich kunnen voordoen niet. Het is immers de vraag of de moeite die nodig is voor het omzeilen van de beveiliging (en kraken van het custom formaat) opweegt tegen de baten. Dat de fysiologische gegevens niet direct gekoppeld zijn aan de drager, maakt het voor buitenstaanders namelijk lastiger om de metingen te herleiden tot personen. Ook hiervoor zijn de nodige inspanningen nodig. Dit maakt het privacyrisico als gevolg van het veiligheidsrisico relatief klein: de kans is klein (maar niet verwaarloosbaar) dat er privacyschendingen optreden door het hacken. Het is nog maar de vraag of er kwaadwillenden zijn die belang hebben bij het (op grote schaal) stelen en hacken van fysiologische gegevens van justitiabelen en wat hun motieven zouden kunnen zijn. Dat is in deze studie niet onderzocht.

6.2.2 Privacyrisico's

Omdat de verzamelde fysiologische gegevens iets over iemands gezondheid kunnen zeggen, is er conform de AVG sprake van bijzondere persoonsgegevens die extra zijn beschermd. Het is daarom zaak om voorzichtigheid te betrachten bij het opslaan en verwerken van dergelijke fysiologische gegevens. Dit betreft onder andere het hanteren van een werkwijze die volledig in lijn is met de privacywetgeving.

Empatica beoogt de privacy van de drager van de band te beschermen door alleen van de gebruiker en niet van de drager direct identificerende gegevens te verzamelen. Dit is in principe een goede maatregel om persoonsgegevens te beschermen en te beveiligen, maar dit betekent niet noodzakelijkerwijs dat de gegevens ook echt anoniem zijn en de privacywetgeving niet meer van toepassing zou zijn op de verwerking van de gegevens. Wanneer de Empatica E4 gebruikt wordt voor onderzoek, behandeling of toezicht is het daarom noodzakelijk om als gebruiker (de verwerkingsverantwoordelijke) een verwerkersovereenkomst met Empatica (de verwerker) af te sluiten. Empatica heeft bij navraag van onze kant ook aangegeven bereid te zijn dergelijke overeenkomsten af te sluiten, en dat maatwerk mogelijk is. Het is van belang om hierin goede afspraken te maken over de doeleinden waarvoor de fysiologische gegevens door Empatica worden verwerkt, wat de bewaartermijn is en met wie ze eventueel gedeeld kunnen en mogen worden. Voor gebruik in de justitiële context zou het bijvoorbeeld te allen tijde mogelijk moeten zijn om alle fysiologische gegevens van justitiabelen volledig en permanent te laten wissen.

De gebruiker dient zich te realiseren dat het niet onmogelijk is om door het combineren van bijvoorbeeld fysiologische gegevens met persoonsgegevens van de gebruiker een drager te identificeren, bijvoorbeeld door gebruik te maken van externe bronnen. Ook als gegevens lekken of onderschept worden, zou het voor derden mogelijk kunnen zijn om deze te koppelen aan personen. Als er meer andere infor-

[94] www.informatiebeveiligingsdienst.nl/product/handreiking-dataclassificatie-2/

matie over de betrokken dragers beschikbaar is, dan wordt de kans op privacy-schendingen groter. Gezien de ontwikkelingen op het gebied van big data (steeds meer data, gemakkelijker en sneller beschikbaar) worden deze risico's in de toekomst alleen maar groter. Wat nu misschien anoniem is, hoeft over een paar jaar niet meer anoniem te zijn (Bargh et al., 2018).

Een ander privacy-gerelateerd nadeel bij het gebruik van de Empatica E4 is dat het niet mogelijk is om selectief meetfuncties aan of uit te schakelen al naar gelang het doel. Het is bijvoorbeeld niet mogelijk om alleen hartslag of huidgeleiding te meten. Om aan te sluiten bij het dataminimalisatie- en doelbindingsbeginsel van de privacywetgeving zou dit wel een gewenste optie zijn. Zo worden er niet meer gegevens verzameld dan nodig. Het is immers denkbaar dat het voor bepaalde onderzoeken, behandelingen of toezichtvormen niet nodig is om alle vier de sensoren metingen te laten doen.

6.3 Belangrijke opties voor fysiologische wearables in de justitiële context

In de voorgaande paragraaf hebben wij de gesignaleerde risico's met betrekking tot dataveiligheid en privacy bij de Empatica E4 besproken. In onze inventarisatie van andere fysiologische wearables die mogelijk geschikt zijn voor gebruik in de justitiële context vonden we verschillende producten die beter presteren op dit gebied. Daarbij viel het op dat er grofweg twee varianten zijn: wearables voor 1) offline (lokaal) gebruik; en 2) online gebruik (met een cloudomgeving). De eerste groep is vooral gericht op onderzoek en/of behandeling in een lab of op een vaste locatie. Deze wearables bieden ook meer configuratiemogelijkheden. De tweede groep is geschikt voor grootschalig onderzoek met veel verschillende deelnemers op verschillende locaties of voor behandeling op afstand. Dit wordt mogelijk gemaakt door een cloudoplossing te bieden. In de justitiële context zouden bij de keuze of gebruikgemaakt wordt van een offline of een online variant het doel, de doelgroep en de meer specifieke context van de desbetreffende toepassing in overweging moeten worden genomen. Ter illustratie hierna twee voorbeelden.

Als het bijvoorbeeld gaat om een onderzoek naar fysiologische maten in relatie tot stressklachten bij gedetineerden, dan zou een offline variant van een wearable wellicht het meest in aanmerking komen. Bij een offline variant is uitgesloten dat gevoelige gegevens van gedetineerden in de cloud terecht komen en worden daarmee verbonden mogelijke risico's op het gebied van dataveiligheid en privacy vermeden. Vanwege de detentie blijven de gedetineerden op dezelfde locatie, in de buurt van de onderzoeker, die de gegevens regelmatig kan downloaden. Bovendien is een offline variant in een penitentiaire inrichting waar internettoegang streng gereguleerd is eenvoudiger toe te passen.

Bij een onderzoek naar een wearable die huidgeleiding meet als hulpmiddel bij agressieregulatie voor jongeren onder reclasseringsbegeleiding, kan wellicht juist worden gekozen voor een online variant. De jongeren zijn niet gedetineerd en bewegen zich vrij, bovendien is het belangrijk dat zij direct zelf feedback krijgen als de spanning (gemeten op basis van huidgeleiding) oploopt, zodat zij zich daarvan meer bewust worden en bijvoorbeeld tijdiger een time-out kunnen nemen. De wearable moet klein en licht zijn en er aantrekkelijk uitzien (anders gebruiken jongeren hem niet lang). Ook moet deze een schermpje hebben en idealiter een geluids- of trilfunctie die een duidelijk signaal afgeeft als de spanning oploopt. Op basis van de

functies die de wearable voor dit onderzoeksdoel moet hebben en de context (zich vrij bewegende jongeren) ligt de keuze voor een online variant voor de hand. Wat betreft de doelgroep wegen privacy en veiligheid van gegevens ook hier zwaar. Daarom zou bij de keuze voor een online wearable de vraag of die aspecten goed zijn geborgd centraal moeten staan.

Op basis van de analyses in de voorgaande hoofdstukken destilleren wij voor zowel de offline als de online gebruiksvariant een aantal aspecten die van belang zijn bij de keuze van een wearable die gebruikt wordt in de justitiële context, en specifiek om gegevens te verzamelen bij justitiabelen.

Offline gebruik

1 Optie om de gegevens volledig lokaal op te slaan, te analyseren en te beheren.
2 Optie om de gegevens versleuteld of geanonimiseerd op de wearable op te slaan of op een andere manier te beveiligen.

Online gebruik

3 Opties om de gegevens te beveiligen bij opslag in de cloud, transport naar de cloud en toegang tot de cloud (bijvoorbeeld versleutelde verbindingen, sterke wachtwoorden, twee-factor-authenticatie).
4 Een verwerkersovereenkomst met de cloudprovider die voldoet aan de privacywetgeving.

Voor gebruik in de justitiële context is een gedegen analyse vooraf van de privacy- en informatiebeveiligingsrisico's essentieel. Dit sluit ook aan bij het beginsel van *privacy by design*. Daarbij is het bijvoorbeeld ook wenselijk om selectief meetfuncties aan of uit te kunnen schakelen, zodat voldaan kan worden aan het dataminimalisatie- en doelbindingsbeginsel van de privacywetgeving. De verwerkingsverantwoordelijke (in dit geval de gebruiker) heeft een verantwoordingsplicht om aan deze beginselen te voldoen en moet dit ook kunnen aantonen.

Dataveiligheid en privacy zijn echter niet de enige wenselijke kenmerken voor wearables in de justitiële context. Redenen voor het gebruik van wearables zijn bijvoorbeeld ook het gebruiksgemak en de mogelijkheid om het meten van relevante gegevens in het dagelijks leven te integreren. Aantrekkelijkheid van de wearable is hiervoor van groot belang. Daarnaast biedt de mogelijkheid van feedback aan de drager in sommige gevallen een grote meerwaarde voor de toepassing van de wearable, bijvoorbeeld bij de behandeling van of het toezichthouden op justitiabelen.

Zoals in hoofdstuk 1 vermeld heeft DJI voor zijn proeftuinen om meerdere redenen gekozen voor de Empatica E4. De eerste reden is dat de Empatica E4 op dat moment de enige wearable was die zowel hartslag als huidgeleiding en beweging kon meten. De tweede reden is dat de Empatica E4 draagvlak had bij collega-onderzoekers met betrekking tot de betrouwbaarheid van de metingen (in vergelijking tot een 'gouden standaard' zoals de VU-AMS). Een derde reden was dat de servers van Empatica waarop de gegevens worden bewaard, destijds in Europa (Italië) stonden. Dit zou een waarborg bieden voor het voldoen aan Europese privacyregelgeving.

Zoals eerder aangegeven blijkt uit de beknopte vergelijking dat er verschillende wearables verkrijgbaar zijn die betere waarborgen dan de Empatica E4 bieden wat betreft veiligheid van gegevens en privacy voor gebruik in de justitiële context, onder andere doordat ze lokaal te gebruiken zijn of betere beveiligingsmaatregelen treffen, en daarnaast redelijk tot goed toepasbaar zijn in het dagelijks leven. Dit zijn

bijvoorbeeld de *EcgMove 4* of *Moodmetric* voor offline gebruik en de *Apple Watch* voor online gebruik. Deze wearables beiden echter minder uitgebreide meetfuncties dan de Empatica E4, doordat het hiermee niet mogelijk is huidgeleiding te meten. De *EcgMove 4* in combinatie met de *EdaMove 4* doet dit laatste wel, maar is dan weer minder bruikbaar door het gebruik van plakkers. Geen van de gevonden en bekeken wearables voldoet vooralsnog aan alle eisen (offline optie of goede beveiliging en verwerkersovereenkomst bij online gebruik, minstens dezelfde sensoren als de Empatica E4, gebruiksgemak en draagbaarheid). In paragraaf 6.4.2 geven we enkele aanbevelingen om in de toekomst te kunnen werken met fysiologische wearables die zoveel mogelijk van de voor gebruik in een justitiële context benodigde kenmerken hebben.

6.4 Conclusies en aanbevelingen

6.4.1 Conclusies

Uit dit casusonderzoek (met name uit de beknopte vergelijking met andere wearables in hoofdstuk 4) komt naar voren dat de Empatica E4 een van de weinige draagbare wearables is die zowel hartslag als huidgeleiding kan meten, maar dat deze wel risico's kent op het gebied van dataveiligheid en privacy. Er zijn wearables beschikbaar die beter presteren wat betreft dergelijke risico's. De belangrijkste risico's van de Empatica E4 zijn:

- De verzamelde fysiologische gegevens gaan automatisch naar de online omgeving van de fabrikant, lokaal gebruik van de polsband is niet (gemakkelijk) mogelijk. Door het gebruik van een online omgeving, is het nodig om een verwerkersovereenkomst met Empatica af te sluiten die aan de geldende privacywetgeving voldoet, met betrekking tot de verwerking van de gegevens door Empatica (onder andere over opslag van, (her)gebruik van en toegang tot de gegevens en bewaartermijnen).
- De mate van beveiliging van de gegevens kan beter.

Uit de beknopte vergelijking van de Empatica E4 met andere wearables komen twee varianten naar voren: een offline variant en een online variant. Welke variant de voorkeur verdient bij het gebruik van fysiologische wearables in de justitiële context, hangt af van het doel, de doelgroep en de specifieke context van het onderzoek, de behandeling of het toezicht. Een analyse van mogelijke risico's wat betreft dataveiligheid en privacy is daarbij van cruciaal belang.

Voor een wearable in de justitiële context zijn de volgende kenmerken van belang met het oog op dataveiligheid en privacy:

- mogelijkheid tot volledig lokaal gebruik; of
- indien online gebruik (tevens) wenselijk is: adequate beveiligingsmogelijkheden en een verwerkersovereenkomst die voldoet aan de van toepassing zijnde privacywetgeving;
- mogelijkheid tot selectief aan en uitschakelen van individuele meetfuncties.

Daarnaast zijn de volgende kenmerken belangrijk met het oog op functionaliteit en gebruiksgemak (deels afhankelijk van de gewenste toepassing):

- een goed aanbod aan betrouwbare, valide en accurate meetfuncties bijvoorbeeld hartslag, huidgeleiding, beweging en (huid)temperatuur;
- voldoende draagcomfort zodat de wearable gemakkelijk geïntegreerd kan worden in het dagelijks leven;

- mogelijkheid tot een feedbackfunctie (bijvoorbeeld via een app op een ander mobiel apparaat of een schermpje op het device zelf).

6.4.2 Aanbevelingen

Op basis van ons casusonderzoek komen we tot de volgende drie aanbevelingen.

Stimuleer bewustzijn, maar ook verantwoord gedrag, wat betreft risico's voor dataveiligheid en privacy bij medewerkers die wearables gebruiken of ermee willen experimenteren.
Benut de mogelijkheden van fysiologische wearables voor de behandeling en het toezicht ten aanzien van justitiabelen, maar faciliteer dat dit verantwoord gebeurt en zorg dat aan de van toepassing zijnde privacywetgeving wordt voldaan. Zoals in de inleiding vermeld laat eerder verkennend onderzoek zien dat technologische zelfmeetmethoden de potentie hebben om zelfredzaamheid van justitiabelen te vergroten, behandeling te personaliseren, veiligheid in detentie te verbeteren en reclasseringstoezicht te verrijken.

Een eerste stap naar een goede omgang met dataveiligheid en privacy is dat gebruikers van wearables met sensoren in de justitiële context zich bewust zijn van waar mogelijke risico's liggen. Het merendeel van de kleine groep professionele gebruikers die voor dit casusonderzoek is bevraagd, geeft er blijk van zich van dergelijke risico's bewust te zijn. De in de inleiding genoemde 'privacy paradox' lijkt voor deze groep echter ook op te gaan: er is bewustzijn van de risico's, maar toch wordt de wearable (de Empatica E4) gebruikt en is men er redelijk tevreden over. Dit heeft er waarschijnlijk ook mee te maken dat er weinig of geen betere alternatieven voorhanden zijn.

Wettelijk gezien zijn de gebruikers als verwerkingsverantwoordelijke verplicht om de naleving van de privacywetgeving aan te tonen. De gebruikers van een wearable hebben met hun gedrag dan ook een belangrijke rol in het veilig omgaan met de verzamelde gegevens. Zelfs als de fabrikant hierin steken laat vallen. Zo kan bij de Empatica E4 gebruikgemaakt worden van de beperkte mogelijkheden die er zijn tot extra beveiliging. Het account kan beveiligd worden met een sterk wachtwoord (dit wordt door Empatica zelf niet afgedwongen). Ook kan de gebruiker, de sessies van dragers zo snel als mogelijk verwijderen uit het gebruikersaccount. De gegevens zijn dan voor Empatica niet meer gekoppeld aan de gebruiker; dit maakt het herleiden van de gegevens naar de drager lastiger. De gegevens kunnen voor verdere analyse dan eerst gedownload worden naar de eigen computer van de gebruiker en vervolgens uit de Empatica Connect-omgeving verwijderd worden. De gebruiker kan de gedownloade gegevens vervolgens op de eigen computer analyseren en visualiseren met software van een andere aanbieder. Ook kan de gebruiker ervoor zorgen dat het aantal sessies per drager zo beperkt mogelijk is (niet meer sessies meten dan nodig). Parameters die voor het meetdoel niet nodig zijn zouden ook direct verwijderd kunnen worden (bijvoorbeeld wel hartslag bewaren, maar temperatuurmetingen verwijderen). Dit laatste is in lijn met het dataminimalisatie- en doelbindingsbeginsel uit de privacywetgeving.

Voer voorafgaand aan de keuze van een wearable een risicoanalyse uit ten aanzien van die wearable en pas de principes van privacy by design toe.
Als men een wearable wil gebruiken in de justitiële context, is het aan te bevelen om eerst een risicoanalyse uit te voeren op de eerder vermelde punten van dataveiligheid en privacy. Dit past ook bij het begrip *privacy by design*: al in een vroeg

stadium (bij de opzet van een onderzoek of pilot, of nog beter bij het ontwikkelen van een wearable) aandacht besteden aan en rekening houden met privacy. Dit kan onder andere door het uitvoeren van een DPIA en/of een Quickscan Informatiebeveiliging. Het is aan te bevelen hierbij de Privacy Officer (PO) en/of Chief Information Security Officer (CISO) van de organisatie(s) te betrekken. Er kunnen meerdere wetten relevant zijn voor verschillende soorten gebruik van wearables. Daarbij komt dat het toepassen van de verschillende wettelijke regels specifieke expertise vergt. Daarom is er hier geen pasklaar antwoord te geven op de vraag of en hoe fysiologische gegevens verzameld mogen worden en welke (beveiligings)maatregelen nodig zijn. Wel wijzen we in dit rapport op een aantal aandachtspunten.

De eerste is dat bij het gebruik van een cloudomgeving waarin fysiologische gegevens worden opgeslagen, het verplicht is om een verwerkersovereenkomst met de cloudprovider af te sluiten. Ook hierbij is het verstandig de PO te betrekken. Als de risico's te groot zijn, als de verwerker niet akkoord gaat met de in de overeenkomst gestelde voorwaarden, of als er om een andere reden niet aan de privacywetgeving kan worden voldaan, dan is het af te raden met het instrument te werken. Tenzij het instrument door iemand met voldoende technische kennis zodanig kan worden aangepast dat de risico's worden ondervangen (door het bijvoorbeeld geschikt maken voor uitsluitend lokaal gebruik).

Bij de verwerking van persoonsgegevens is het uitvoeren van een DPIA in het kader van de privacywetgeving in veel gevallen verplicht. Als het gaat om bijzondere persoonsgegevens (zoals de met een wearable verzamelde fysiologische gegevens), is er een grondslag voor verwerking nodig, anders is verwerking verboden. Een uitzondering op het verwerkingsverbod is onder andere het uitvoeren van wetenschappelijk onderzoek in het algemeen belang. Ook het verkrijgen van uitdrukkelijke toestemming van de dragers vormt een uitzondering op dit verbod, mits deze toestemming in vrijheid is gegeven. Ook dan blijft de gebruiker echter verantwoordelijk voor een goede bescherming van de verzamelde persoonsgegevens. Uiteraard is het in alle gevallen ethisch gezien aan te bevelen potentiële deelnemers aan onderzoek of (experimentele) behandelingen goed te informeren over wat er gebeurt met hun persoonsgegevens.

Ook bij het opzetten van proeftuinen en pilots dient aan de privacywetgeving te worden voldaan. Het is dan onder andere van belang een DPIA uit te voeren, de verwerkingen vast te leggen in een verwerkingsregister en eventueel een verwerkersovereenkomst met de verwerkers af te sluiten. In sommige gevallen is het daarnaast van belang om schriftelijke toestemming van de deelnemers te verkrijgen (bijvoorbeeld als een andere grondslag voor de verwerking ontbreekt of als het om medisch-wetenschappelijk onderzoek gaat), en wellicht ook een ethische toetsing zoals besproken in paragraaf 1.3 te laten uitvoeren.

In de justitiële context zou daarom concreet de volgende werkwijze gevolgd moeten worden bij onderzoek, behandeling en toezicht met fysiologische wearables:

- De gebruiker neemt passende technische en organisatorische maatregelen, volgt de principes van *privacy by design*, en kan als verwerkingsverantwoordelijke de naleving van de privacywetgeving aantonen, door onder andere:
  - een verwerkingsregister bij te houden;
  - een DPIA uit te voeren;
  - een verwerkersovereenkomst met de verwerker af te sluiten (indien van toepassing).

- Er wordt zorgvuldig omgegaan met de vaak kwetsbare doelgroep:
  - binnen de doelgroep wordt gevraagd wie de wearable wil dragen (kan niet worden verplicht);
  - de drager wordt geïnformeerd over het doel van het onderzoek, de behandeling of het toezicht, over wat de consequenties zijn van dragen en wat er met de fysiologische gegevens gebeurt, zodat deze geïnformeerd en vrijelijk kan bepalen mee te doen;
  - toestemming van de drager wordt schriftelijk vastgelegd en kan te allen tijde weer worden ingetrokken.

Bij het gebruik voor onderzoeksdoeleinden is ethische toetsing belangrijk maar tijdrovend, vooral een METC-traject, en al helemaal als daarnaast ook de toetsingsprocedure voor een medisch hulpmiddel moet worden gevolgd. Een medisch ethisch toetsingstraject vraagt van de onderzoekers een zeer uitgebreid pakket aan documentatie en veelal moeten de onderzoekers ook een of meer keren voor de commissie verschijnen. Een dergelijk traject kan een half jaar tot een jaar in beslag nemen. Het is dan ook aan te raden daarmee ook in de justitiële context rekening te houden in de planning van onderzoeksprojecten.

Pas indien nodig de software van een bestaande wearable aan.
Het is in principe mogelijk om van bestaande wearables de software dusdanig aan te passen dat ze voldoen aan de kenmerken die wenselijk zijn voor toepassing in de justitiële context. Zo is vanuit de universiteit Twente *Sense-IT* ontwikkeld (Derks, Visser, Bohlmeijer, & Noordzij, 2017), een platform dat bestaat uit een applicatie en een *Wear OS*-smartwatch. Hierbij is het theoretisch mogelijk om de gegevens van de wearable lokaal te verzamelen en te analyseren. Op dit moment gebeurt dat echter nog niet. Ook is er een feedback-functionaliteit ontwikkeld (bijvoorbeeld in het promotieproject van Annemieke ter Harmsel[95]).

Het aanpassen van de software van een bestaande wearable zou een interessante en laagdrempelige mogelijkheid kunnen zijn om de gewenste kenmerken te bereiken. Een nadeel bij het specifieke voorbeeld hierboven is dat de meeste smartwatches nog geen huidgeleiding meten. De Empatica E4 blijkt een van de weinige gebruiksvriendelijke wearables met deze functie. Bij de Empatica E4 is het ook mogelijk de software aan te passen voor alleen lokaal gebruik (met de SDK van Empatica). Twee Nederlandse voorbeelden van apps die andere functionaliteiten bieden dan de standaardapp van de fabrikant zijn *GRIP* (werkt nog niet met de Empatica E4) en *HUME* (kan al wel met de Empatica E4 gebruikt worden). Bij de Empatica E4 ontbreekt dan echter nog steeds een feedbackfunctie op het scherm die andere wearables wel bieden.

Een nadeel bij het aanpassen van een bestaande (commerciële) wearable kan zijn dat er nog steeds afhankelijkheid is van een commerciële derde partij. Dit kan financiële consequenties hebben. Ook is er een risico dat de productie stopt en dat er dan mogelijk geen ondersteuning en updates meer geboden worden, en het instrument veroudert of de beveiliging verslechtert.

Om volledige regie te hebben over de functionaliteiten en om de aan veiligheids- en privacywaarborgen te voldoen zou het ministerie van Justitie en Veiligheid zelf kunnen investeren in het laten (door-)ontwikkelen van een (bestaande) wearable.

[95] www.inforsa.nl/onderzoek/onderzoeksprojecten/

Dit kan eventueel in samenwerking met andere ministeries zoals VWS en maatschappelijke partners. Zo kan de mogelijkheid gecreëerd worden om alle gewenste functionaliteiten te integreren in een wearable: zowel hartslag als huidgeleiding kunnen meten, én beschikken over de mogelijkheid van feedback. Dit eventueel in combinatie met meer sensoren specifiek voor medische doeleinden om de toepasbaarheid te vergroten. Ook kunnen veiligheids- en privacywaarborgen dan beter gegarandeerd worden alsook de ondersteuning in de toekomst. Deze wearable zou dan minimaal moeten voldoen aan de in paragraaf 6.3 genoemde kenmerken.

Summary

Data security and privacy when using physiological wearables in the judicial context

A case study with the Empatica E4

Background and research questions

Research shows that technological self-measurement methods have the potential to personalize treatment, improve security in detention, enrich probation supervision and increase the self-reliance of offenders. Nevertheless, there are also serious concerns and risks associated with the use of technological self-measurement methods. For example, it is often unclear what exactly happens with the data after they are collected. Data collected with technological self-measurement methods are often accessible to the manufacturer and may be shared with third parties. The technology itself is also sometimes vulnerable, resulting in the interception or theft of data by third parties. This is certainly not desirable in the judicial context – where security and privacy protection are paramount. Before technological self-measurement methods can be used on a larger scale in the judicial context, it is therefore important to investigate the state of data security regarding self-measurement methods, and to assess what could be done in the judicial context to ensure the security of the collected data and thereby the privacy of those involved.

In this report, we describe a case study on data security and privacy, focusing on *physiological wearables*. These are portable devices that are worn around the wrist or on the body and with which physiological data can be collected by means of sensors. We conducted this case study with a specific wearable: the Empatica E4.

The following questions were answered:

1 What happens to the physiological data of the Empatica E4 after these have been collected by the user with regard to: data storage, data transfer and third party access to the data?
2 What are the risks for the security of the data and for the privacy of the wearer? And how does the Empatica E4 compare to other wearables with respect to the risks and functionality?
3 What are the knowledge, experiences and concerns of professional users of the Empatica E4 regarding data storage, access to data by third parties and privacy?
4 What do the answers to the sub-questions mean for the use of the Empatica E4 and other physiological wearables in the judicial context?

Based on the case study, we make recommendations about how best to deal with the security and privacy of data collected with physiological wearables in the judicial context. Security of the data relates to the security regarding data storage and transmission. In this report, privacy means the protection of the collected (personal) data of the wearer of the physiological wearable against disclosures.

This report mainly discusses the use of wearables for research, treatment or supervision in the judicial context. We distinguish between the user and the wearer. The user (for example a researcher, forensic clinician or probation officer) is the person

who collects, stores, processes, analyses, and deletes the data. Often the user is also the person who purchases the wearable, enters into the agreement with the manufacturer, and provides his or her personal data to the manufacturer (for instance to make an online account). The wearer is the person who wears the wearable and whose physiological data are collected. The wearer can, for example, be a detainee who takes part in scientific research.

Methods and Limitations

Questions 1 and 2 were answered by carrying out desk research. Information and documentation about security and privacy was searched on the Empatica-website and additional questions were asked via email to Empatica. An account was created to try out the storage, transfer and use of data with the Empatica E4 in practice. For the comparison of the data security and privacy of the Empatica E4 with those of other wearables (part of question 2), relevant wearables were searched by consulting various internet sources using systematic search terms and by questioning experts. For the analysis, we only selected wearables that, like the Empatica E4, can measure skin conductance and/or heart rate, and ideally also movement and/or skin temperature. Question 3 was answered by means of a short survey among ten professional users of the Empatica E4, and question 4 was answered on the basis of the findings regarding the first three questions.

In this study we compared the Empatica E4 with a number of other wearables. On the one hand we looked at the functionality offered and on the other hand at the data security and privacy. An important limitation is that this comparison is not exhaustive. A limitation is that we were not able to map all risks relating to data security and privacy for all wearables in detail because we collected the information through public sources like websites. These sources do not always include all details for each wearable. Another limitation is that we investigated the user experiences in a very small sample of ten users (partly because there are few users in the Netherlands). This consultation also took place before the General Data Protection Regulation (GDPR) came into effect and the knowledge of users may have increased in the meantime.

Data security and privacy when using the Empatica E4

The Empatica E4 wristband which contains four different sensors (skin conductance, heart rate, acceleration and skin temperature) can be used in two ways. In streaming mode, the wristband data are displayed directly in real time in an app on a mobile device. This data is then automatically uploaded to the user's E4 Connect account on Empatica's servers. In recording mode, after connecting the Empatica E4 to a computer, the data stored on the wristband are automatically moved to a storage location on the computer and then automatically uploaded to the user's E4 Connect account. The data can be viewed on the E4 Connect website.

Such an environment in which data is not stored locally with the user, but on the servers of a third party, is called a cloud or cloud environment. The data in the cloud are accessible from any device with an internet connection. Empatica not only offers data storage with E4 Connect, but offers a website (also called a dashboard), with which the data can be viewed and managed.

Our case study shows that Empatica has taken several measures to secure the physiological data of the wearers during transport and when storage on Empatica's servers against possible interception by third parties. For example, the data are linked to the user and not to the wearer, are stored in a special format and the data transfer is encrypted. As a result, the physiological data (from the wearer of the wristband) can only be traced back directly to individual persons by the user and not by the manufacturer. Nevertheless, we see various risks regarding the security of the collected data and the privacy of the wearer.

Security risks
The most important security risk is that the physiological data are automatically transferred to the online environment of the manufacturer. Local (offline) use of the wristband is not (easily) possible. Sending data over the internet and storing them in the cloud involves a greater risk of intercepting or stealing data by third parties than a solution that works completely offline and uses local storage. In the case of local offline storage, intercepting or stealing data is more difficult because the storage must first be accessed physically (while the cloud storage can be hacked or attacked remotely). With local use, the user has more flexibility and control over, for example, where the data collected are stored, and data from wearers are not (automatically) shared with an external party. The user is then responsible for adequate security of the devices on which the data are stored and analysed.

Privacy risks
Because the physiological data can say something about a person's health, these belong to a special category of personal data (in the sense of the GDPR) that need to be protected more. These data must therefore be handled with care, in accordance with the (privacy) legislation applicable, in order not to harm the privacy of the wearer. Because the Empatica E4 uses a cloud environment, in which Empatica becomes the processor of the data, it is important to have a (privacy) lawyer conclude a data processing agreement with Empatica. This is mandatory to comply with privacy legislation. After inquiries from our side, Empatica has indicated to be willing to conclude such agreements, and that customization is possible. The agreement should include in which country the data will be stored, who will have access to the data and for how long they will be stored. For use in the judicial context, it should for instance be possible at any time to have all physiological data of wearers such as detainees completely and permanently erased.

Comparison data security, privacy and functionality of the Empatica E4 with other physiological wearables

Several manufacturers have developed wearables for use by professionals in research or treatment. In addition there are consumer wearables available that could also be used for research, treatment or supervision.

What is striking when looking at instruments intended for treatment and research is that there are roughly two variants: 1) wearables or portable devices for use in a lab or at a fixed location; and 2) wearables suitable for larger-scale research and/or remote treatment, with many different participants in different locations. Offline solutions are available for the first group. These wearables also offer users more configuration options, allowing them to determine which measurements are collected and where they are stored. The user is then responsible for taking measures to protect the data. Due to the many possibilities, some of these wearables seem to

require more technical expertise to use. In the second group of wearables, it is striking that all providers, like Empatica, opt for a cloud solution. This makes it easier for users to conduct larger studies. In addition, participation in a study is easier for the wearers: it is not necessary to come to a lab, the band can be worn at home for a long time (some products are even waterproof), and it takes little effort to send the measurements to the user because this is largely automated. For some products, the wearers can also gain (real time) insight into their own measurements by using a mobile app (none of these products have a screen on the wearable itself to show physiological data in real time).

The use of consumer wearables, mostly smartwatches, for research or treatment is also possible. This has the advantage that the wearer himself can keep an eye on the measurements (by using the directly readable screen and/or using an app) and at the same time use the other functionalities of the smartwatch. A disadvantage for the use of these wearables in the judicial context is that these instruments currently have (much) fewer sensors than the products aimed at professionals. For example, there are not many smartwatches that can measure skin conductance, but many smartwatches do contain a heart rate sensor. Furthermore, the sensors may not always be validated. These smartwatches generally use the cloud to store physiological data.

Our comparison showed that there are not many wearables on the market that, like the Empatica E4, both provide a combination of several different physiological sensors (both heart rate and skin conductance sensor), and are easily usable. There are instruments that do contain these sensors, but these make use of (less user-friendly) patches. However, several instruments do score better than the Empatica E4 in terms of: the possibility to use the instrument completely locally without the need for the cloud or a cloud service with better security measures.

Experiences of professional users

Although a majority of the users of the Empatica E4 have read the privacy statement beforehand, a third of the users have not. It is therefore not surprising that most of them do not know or answer neutrally to a question about how the manufacturer of the wearable deals with data storage and access. Hardly any user knows where and for how long the collected data are stored. There are also concerns about access by third parties and misuse of data. In conclusion, users are concerned about the security of data storage and access, but nevertheless use the wearable. This is called the 'privacy paradox' and may be due to the fact that there are few alternatives available.

The use of physiological wearables in the judicial context

Based on our case study, we distil a number of aspects and recommendations that are important for the use of physiological wearables in the judicial context and more specifically the collection of physiological data from detainees, forensic patients, parolees or other subjects within the criminal justice system.

Important options for physiological wearables in the judicial context
The following characteristics are important for a wearable in the judicial context with respect to data security and privacy:
- the possibility of full local use; or
- if online use is (also) desirable: adequate security options and a data processing agreement that complies with the applicable privacy legislation;
- the possibility to selectively switch on and off individual measurement functions.

In addition, with respect to functionality and ease of use (partly depending on the desired application), it is important to have the following characteristics:
- a good range of reliable, valid and accurate measurement functions such as heart rate, skin conductance, movement and (skin) temperature;
- sufficient wearing comfort so that the wearable can be easily integrated into everyday life;
- the possibility of a feedback function (for example via an app on another mobile device or via a screen on the device itself).

The choice of a particular instrument and its suitability depends on the precise purpose (for example: which measuring functions are required, whether direct feedback to the wearer via a screen is required, etc.). Our research reveals two variants: an offline variant and an online variant. Which variant is preferred in the judicial context depends on the aim, subjects and specific context of the research, treatment or supervision. An analysis of possible risks regarding data security and privacy is in all cases of crucial importance.

Recommendations
Based on this case study, we have the following three recommendations.

1 *Encourage awareness, but also responsible behaviour, regarding data security and privacy risks among employees who use physiological wearables in pilots, scientific research, treatment or supervision.*
Use the possibilities of physiological wearables in research and for treatment and supervision, but facilitate that this is done responsibly and ensure that the applicable privacy legislation is complied with. From a legal point of view, users are required as controllers to demonstrate that data are processed in accordance with privacy legislation. Users of wearables therefore play an important role in handling the collected data safely (for example: protecting data with a strong password, erasing data from the cloud environment as quickly as possible, not measuring more aspects than necessary).

2 *Before selecting a wearable, perform a risk analysis with regard to that wearable and apply the principles of privacy by design.*
The ex-ante risk analysis should focus on the above-mentioned issues of data security and privacy. It is recommended to consult a Privacy Officer and/or Chief Information Security Officer. This also fits with the concept of privacy by design: paying attention to and taking privacy into account in the early phases of a project. In the judicial context, it is therefore advisable to use the following concrete method for research, treatment or supervision with physiological wearables:
The user takes appropriate technical and organizational measures, follows the principles of privacy by design and, as controller, demonstrates compliance with privacy legislation by among other things:
   - maintaining a record of processing activities;
   - conducting a Data Protection Impact Assessment (DPIA);

- concluding a data processing agreement with the data processor (if applicable).

The often vulnerable target group is handled with care:

- members of the group of interest are asked if they want to take part and wear the wearable (this cannot be compulsory);
- the wearer is informed about the purpose of the research study, treatment or supervision, about the consequences of wearing and what happens to the physiological data, so that he or she can make an informed decision whether or not to participate;
- consent of the wearer is recorded in writing and can be withdrawn at any time.

3 *If necessary, invest in adapting the software of an existing wearable in such a way that it meets the characteristics that are desirable for use in the judicial context.*

There are various practical examples of research projects in the Netherlands in which the software of the wearables has been adapted. A disadvantage of adapting an existing (commercial) wearable may be that there is still dependence on a commercial third party. This can have financial consequences and there is also a risk that production will stop and support and updates may cease, and the instrument will become obsolete or security will deteriorate. In order to have full control over the functionalities and to meet the security and privacy requirements, the Ministry of Justice and Security could itself invest in developing or continuing the development of an (existing) wearable.

Literatuur

Aoyama, T., Koike, M., Koshijima, I., & Hashimoto, Y. (2013). A unified framework for safety and security assessment in critical infrastructures. *Safety and Security Engineering V*, *134,* 67-77. DOI:10.2495/SAFE130071.

Article 29 Data Protection Working Party (2017). Opinion 2/2017 on data processing at work. Geraadpleegd op 18 juli 2019: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

Bargh, M.S., Meijer, R.F., & Vink, M. (2018). *On statistical disclosure control technologies: For enabling personal data protection in open data settings.* Den Haag: WODC. Cahier 2018-20.

Barrios, L., Oldrati, P., Santini, S., & Lutterotti, A. (2019, May). Evaluating the accuracy of heart rate sensors based on photoplethysmography for in-the-wild analysis. In *Proceedings of the 13th EAI International Conference on Pervasive Computing Technologies for Healthcare* (pp. 251-261).

Barth, S., de Jong, M.D.T., (2017). The privacy paradox: Investigating discrepancies between expressed privacy concerns and actual online behavior: A systematic literature review. *Telematics and Informatics, 34(7)*, 1038-1058.

Borrego, A., Latorre, J., Alcañiz, M., & Llorens, R. (2019, July). Reliability of the Empatica E4 wristband to measure electrodermal activity to emotional stimuli. In *2019 International Conference on Virtual Rehabilitation (ICVR)* (pp. 1-2). IEEE.

Burghouts, A. (2015). *Veilig omgaan met eHealth – dit zeggen de experts.* Den Haag: Nictiz.

Cornet, L.J.M., Mandersloot, M.N.A., Pool, R.L.D., & Kogel, C. H. de (2017). *De 'zelfmetende' justitiabele: Een verkennend onderzoek naar technologische zelfmeetmethoden binnen justitiële context.* Den Haag: WODC. Cahier 2017-17.

Cosoli, G., Spinsante, S., & Scalise, L. (2020). Wrist-worn and chest-strap wearable devices: Systematic review on accuracy and metrological characteristics. *Measurement*, 107789.

Derks, Y.P., Visser, T.D., Bohlmeijer, E.T., & Noordzij, M.L. (2017). MHealth in Mental Health: How to efficiently and scientifically create an ambulatory biofeedback e-coaching app for patients with borderline personality disorder. *International Journal of Human Factors and Ergonomics*, 5(1), 61-92.

Drongelen, A. van, Bruijn, A. de, Roszek, B., & Vonk R. (2019). *Apps under the medical devices legislation*. Geraadpleegd op 18 juli 2019: www.rivm.nl/publicaties/apps-under-medical-devices-legislation-apps-onder-medische-hulpmiddelen-wetgeving.

European Data Protection Board (2020a). *Statement on privacy implications of mergers*. Geraadpleegd op 7 juli 2020: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statement_2020_privacyimplicationsofmergers_en.pdf.

European Data Protection Board (2020a). *Statement on the Court of Justice of the European Union Judgment in Case C-311/18*. Geraadpleegd op 24 september 2020: https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en.

Hengst, B., Pelt, V. van, Postema, T., & Ekker, A. (2014). *Zelfmetingen en de Nederlandse gezondheidszorg*. Den Haag: Nictiz. White paper.

ICTRecht (2019). *Advies opslag medische data in de cloud.* Z.pl.: Z.uitg.

Kogel, C.H. de (2019). Technologische hulpmiddelen bij toezicht op delinquenten in de samenleving. *Justitiële verkenningen,* (3), 78-95.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, *64*, 122–134. DOI:10.1016/j.cose.2015.07.002.

Looff, P. de, Noordzij, M.L., Moerbeek, M., Nijman, H., Didden, R., & Embregts, P. (2019). Changes in heart rate and skin conductance in the 30 min preceding aggressive behavior. *Psychophysiology,* e13420. DOI: 10.1111/psyp.13420.

Lam, B., Hong, J.Y., Ong, Z.T., & Gan, W.S. (2018). Reliability of wrist-worn sensors for measuring physiological responses in soundscape assessments. *INTER-NOISE and NOISE-CON Congress and Conference Proceedings*, *258(3)*, 4630-4639. Institute of Noise Control Engineering.

Lier, H.G. van, Pieterse, M.E., Garde, A., Postel, M.G., de Haan, H.A., Vollenbroek-Hutten, M.M., ... & Noordzij, M.L. (2019). A standardized validity assessment protocol for physiological signals from wearable technology: Methodological underpinnings and an application to the E4 biosensor. *Behavior research methods*, 1-23.

McCarthy, C., Pradhan, N., Redpath, C., & Adler, A. (2016). Validation of the Empatica E4 wristband. *2016 IEEE EMBS International Student Conference (ISC)*, 1–4. DOI: 10.1109/EMBSISC.2016.7508621.

Menghini, L, Gianfranchi, E, Cellini, N, Patron, E, Tagliabue, M, & Sarlo, M. (2019). Stressing the accuracy: Wrist-worn wearable sensor validation over different conditions. *Psychophysiology, 56*(11), :e13441. https://doi.org/10.1111/psyp.13441.

Ollander, S., Godin, C., Campagne, A., & Charbonnier, S. (2016, October). A comparison of wearable and stationary sensors for stress detection. In *2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* (pp. 004362-004366). IEEE.

Ossebaard, H.C., Bruijn, A.C.P. de, Gemert-Pijnen, J.E. van, & Geertsma, R.E. (2012). *Risks related to the use of eHealth technologies: An exploratory study.* RIVM Report 360127001/2012.

Pietilä, J., Mehrang, S., Tolonen, J., Helander, E., Jimison, H., Pavel, M., & Korhonen, I. (2017). Evaluation of the accuracy and reliability for photoplethysmography based heart rate and beat-to-beat detection during daily activities. *EMBEC & NBC 2017*, 145–148. DOI: 10.1007/978-981-10-5122-7_37.

Ragot M., Martin N., Em S., Pallamin N., Diverrez J.M. (2018) Emotion recognition using physiological signals: Laboratory vs. wearable sensors. In T. Ahram & C. Falcão (red.), *Advances in human factors in wearable technologies and game design: AHFE 2017: Advances in intelligent systems and computing* (vol. 608; pp. 15-22). Z.pl.: Springer, Cham.

Rosanio S. (2018). *Adviesrapport quantified self: Proeftuin fase 2*. Den Haag: DJI.

Saganowski, S., Kazienko, P., Dzieżyc, M., Jakimów, P., Komoszyńska, J., Michalska, W., ... & Ujma, M. (2020). *Review of consumer wearables in emotion, stress, meditation, sleep, and activity detection and analysis*. arXiv preprint arXiv:2005.00093.

Schuurmans, A., de Looff, P., Nijhof, K. S., Rosada, C., Scholte, R., Popma, A., & Otten, R. (2020). Validity of the Empatica E4 wristband to measure Heart Rate Variability (HRV) parameters: A comparison to electrocardiography (ECG). *Journal of medical systems, 44*(11), 190. https://doi.org/10.1007/s10916-020-01648-w.

Shcherbina, A., Mattsson, C. M., Waggott, D., Salisbury, H., Christle, J.W., Hastie, T., Wheeler, M.T., & Ashley, E.A. (2017). Accuracy in wrist-worn, sensor-based measurements of heart rate and energy expenditure in a diverse cohort. *Journal of personalized medicine, 7*(2), 3. https://doi.org/10.3390/jpm7020003.

Taj-Eldin, M., Ryan, C., O'Flynn, B., & Galvin, P. (2018). A review of wearable solutions for physiological and emotional monitoring for use by people with autism spectrum disorder and their caregivers. *Sensors*, *18*(12), 4271.
Verbruggen, P., & Wolters, P.T.J. (2017). Consument en cybersecurity: Een agenda voor Europese harmonisatie van zorgplichten. *Tijdschrift voor consumentenrecht & handelspraktijken, (1),* 20-29.

Bijlage 1 Leden leescommissie

Dr. P. de Looff	Fivoor, Expertisecentrum De Borg
Dr. M.L. Noordzij	Universiteit Twente
Drs. A.W.M. Eijken	Directoraat-Generaal Straffen en Beschermen, Directie Sanctietoepassing en Jeugd, Ministerie van Justitie en Veiligheid
Drs. E. Eilering	Dienst Justitiële Inrichtingen, Ministerie van Justitie en Veiligheid
Drs. S. Rosanio MBA	Directie Informatievoorziening en Inkoop, Ministerie van Justitie en Veiligheid
Dr. E.C. Leertouwer	Wetenschappelijk Onderzoek- en Documentatie-centrum

Bijlage 2 Gebruikersenquête Empatica E4

Beste collega, 6 april 2018

Vanuit het WODC doen wij onderzoek naar de veiligheid van dataopslag en -verwerking van technologische zelfmeetmethoden. Daartoe hebben we één casus device geselecteerd; de Empatica E4. Behalve in technologische en juridische informatie over het device, zijn we ook geïnteresseerd in de meningen en ervaringen van gebruikers van de Empatica E4 als het gaat om dataopslag en veiligheid.
Graag leggen we onderstaande vragen aan u voor.

Dear colleague,
The WODC currently investigates data security and storage of self-measurement methods. For this research, we have selected one case of a self-measurement method: the Empatica E4. We would like to better understand what users' opinions and experiences are with regard to Empatica's privacy policy and data storage. Therefore we would like to ask you to complete the following questions.

Privacy policy		Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
1	I have read Empatica's privacy policy						
2	I understand Empatica's privacy policy						
3	I agree with Empatica's privacy policy						
4	If you do not (entirely) agree, can you say with which aspects you do not agree?						
Data quality							
5	I worry that data I, measured with the Empatica wristband are not accurate						
6	I worry that data I measured with the Empatica wristband are biased						
7	I worry that data I measured with the Empatica wristband are not complete						
8	If you worry about any of these aspects (accurateness, bias, completeness) can you say why?						

Data entry and privacy		Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
9	I am aware that by using the Empatica wristband, I disclose information to Empatica vendor.						
10	I am concerned that personal information (e.g. age, location, etc. in combination with data measured with the wristband) I disclose to Empatica vendor could be misused.						
11	I am concerned that Empatica vendor can share my personal information (age, location, etc. in combination with data measured with the wristband) with third-parties without my consent.						
12	I am concerned about providing my personal information (age, location, etc. in combination with data measured with the wristband) to Empatica vendor because it could be used in a way I did not foresee.						
13	I have the option to influence what part of my personal information (age, location, etc. in combination with data measured with the wristband) is disclosed to Empatica vendor.						
14	Altogether, I am satisfied with how Empatica vendor deals with the privacy aspects regarding personal information (like age and location) and data collected with the wristband.						
15	Do you have any further remarks about your (dis)satisfaction with privacy aspects of data entry when using the Empatica wristband?						

Data storage		Strongly disagree	Disagree	Neutral	Agree	Strongly agree	Don't know
16	I know which part of the data collected when I use the Empatica wristband is stored by Empatica vendor.						
17	I can influence which part of the data collected when I use the Empatica wristband is stored by Empatica vendor.						
18	I know in which location(s) the data collected when I use the Empatica wristband are stored.						
19	I can influence the location(s) of storage of the data collected when I use the Empatica wristband.						
20	I know for how long the data collected when I use the Empatica wristband are stored.						
21	I can influence the duration of the storage period of the data collected when I use the Empatica wristband.						
22	I am satisfied with how Empatica vendor stores the data collected when I use the Empatica wristband.						
23	Do you have any further remarks about your (dis)satisfaction with data storage by Empatica vendor?						

We would appreciate to know your name and function, but you can also choose to stay anonymous

Name:

Function:

Bijlage 3 Vragen fabrikant Empatica E4

Aug 1 2019

The WODC (Research and Documentation Centre of the Dutch Ministry of Justice and Security) currently investigates data security and storage of wearable physiological measurement methods. For this research, we have selected one wearable as a case-study: the Empatica E4. We are investigating what is currently known from the manufacturer and user (or researcher) concerning the storage of the data, the transport of the data and the access to the data. Our goal is to map the risks for the security of the data and for the privacy of the user and study participants wearing the device. This research is carried out by analyzing the privacy policy of the E4 (www.empatica.com/connect/privacy.php) and additional information on your website. In order to fully answer our research questions, we would appreciate if you could provide us with some additional information that we couldn't find on your website. Therefore we would like to ask you to answer the following questions.

1 Your privacy policy states that 'Empatica does not collect personal data from people physically wearing the Device'. The data housed in E4 connect cannot be matched with the individuals physically wearing the device. Are we correct to assume that the privacy policy only applies to the personal data of the user (i.e., the name and contact details), and, hence, does not concern the physiological data?
2 Does Empatica have access to the data housed in E4 connect (i.e., the physiological signals)?
3 If so, how does Empatica use these data and for what purposes?
4 Who can have access to these data (third-party recipients) and for what purposes?
5 An E4 connect account can be deleted, this disassociates the sessions recorded from the email address, but does Empatica keep a record of these sessions?
6 What are the data retention periods for the data housed in E4 connect?

Aug 21 2020

The WODC (Research and Documentation Centre of the Dutch Ministry of Justice and Security) is currently investigating security and privacy aspects of using wearables in the judicial context. In a typical use case scenario, delinquents or offenders would wear wearables and their physiological measurements would be used for behavioral research, treatment or supervision by an employee of the ministry. In this context, we are investigating how the physiological data obtained through wearables should be stored and transported, and who may be allowed access to these data, such that the ministry adheres to the General Data Protection Regulation (GDPR) and respects the privacy of the participants.

For our research, we have selected one wearable as a case-study: the Empatica E4. In order to fully answer our research questions, we would appreciate if you could provide us with some additional information that we couldn't find on your website. Therefore we would like to ask you to answer the following questions.

1 When the E4 is used by the ministry of Justice, the ministry would act as the data processor. As the physiological data are stored in the cloud (E4 Connect), Empatica would act as a data controller. To comply with GDPR the ministry would be required to have a Data Processing Agreement with Empatica that is in accordance with the GDPR. Do you have experience with such an agreement? Are you willing to sign such an agreement? Do you already have such agreements with other parties?
2 Concerning the data housed in E4 Connect:
   a Does Empatica have access to the data housed in E4 Connect (i.e., the physiological signals)?
   b If so, how does Empatica use these data and for what purposes?
   c Who can have access to these data (third-party recipients) and for what purposes?
   d An E4 Connect account can be deleted, this disassociates the sessions recorded from the email address, but does Empatica keep a record of these sessions?
   e What are the data retention periods for the data housed in E4 Connect?