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.