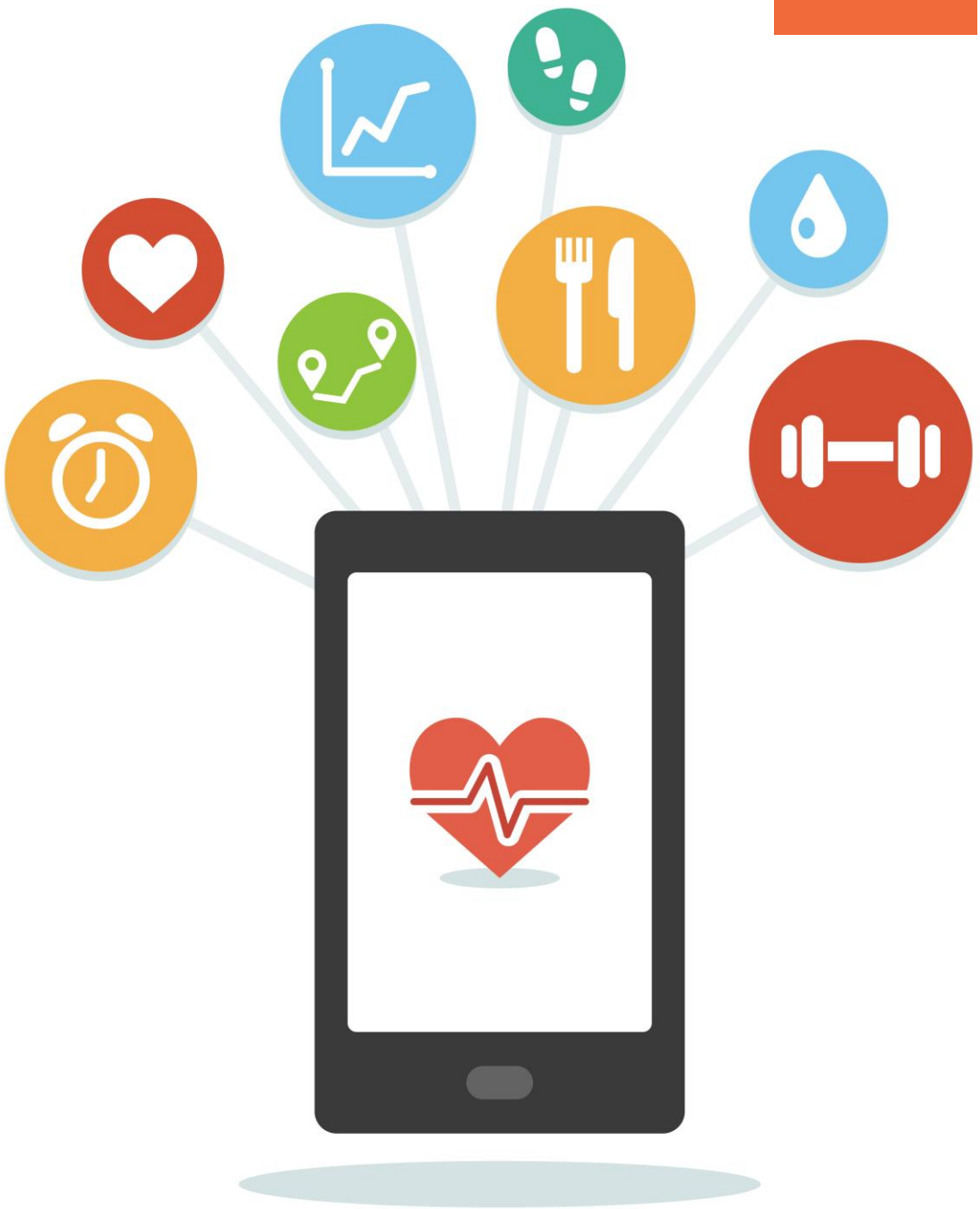

Hva gjør dere med dataene mine?

En kartlegging av hjemmetester innen helse

GPEN-sveipet, september 2016

Datatilsynet

Oppsummering og hovedfunn

Datatilsynet har sjekket personverninformasjonen i seks hjemmetestprodukter koblet opp mot smarttelefon. Produktene måler blodtrykk, blodsukker (typisk brukt av diabetikere) og såkalte oksymeter/pulsoksymeter som måler oksygenmetning i blodet og puls (aktuelt for kolspasienter). Vi har sett på produkter som er lett tilgjengelig for norske forbrukere. Kartleggingen, eller «sveipet» som vi kaller det, er del av et internasjonalt samarbeidsprosjekt med 25 deltakende tilsynsmyndigheter.

Vi har funnet varierende og i hovedsak for dårlig personverninformasjon på de seks produktene vi testet:

- Fem av seks produkter får stryk fordi de ikke forklarer hvordan personopplysningene blir samlet inn, brukt og delt på en tilfredsstillende måte.
- Fire av de seks produktene hadde ingen personvernerklæring.
- Det var varierende kvalitet på informasjon fra produkt til produkt. Resultatene spenner fra ingen informasjon til en del relevant og god informasjon.
- Ingen av produktene forklarte på en god måte hvordan personopplysningene til brukeren blir lagret.
- Ingen av produktene forklarte hvordan brukerne kan slette egne personopplysninger.

Brukervennlig utstyr, men ikke brukervennlig informasjon. Det er enkelt å komme i gang, installere apper, ta tester og å lese av resultater. Det er imidlertid *vanskelig* for brukeren å finne informasjon om hva som skjer med personopplysningene hennes.

Kjøp først, ta stilling senere? Selvråderett er et viktig prinsipp i et godt personvern, og informasjon er en forutsetning for bevisste valg. Vi erfarte at det på kjøpstidspunktet er nesten umulig å vite om produktet ivaretar personvernet ditt på en god måte. Eventuell informasjon kommer ofte når du installerer appen på telefonen din, og det kreves ofte en betydelig leteinnsats av deg som bruker.

Datasikkerhet. Alle produktene hadde mulighet for videreformidling av testresultater per e-post. Et av produktene gav mulighet for å dele testresultater på Twitter og Facebook direkte fra appen. Flere av tjenestene var penset inn på kontakt med helsevesenet. Å sende sensitive personopplysninger (helsedata inkludert) per e-post til og fra helseinstitusjoner er ikke tillatt ifølge personvernregelverket.

Innledning

I dag trenger du ikke å gå legen for å sjekke blodtrykket ditt eller for å ta en rekke andre helserelaterte tester. Du kan gjøre det hjemme. Eller hvor du måtte ønske. Alt du trenger er et testapparat som kommuniserer med smarttelefonen din, og en applikasjon (app) som du laster ned på telefonen. Eller kanskje bare en app på smarttelefonen. I tillegg til å være en datamaskin har telefonene etter hvert fått svært avanserte sensorer.

Det er stor forskjell mellom hvordan en test på legekontoret og hjemmetester av denne typen ivaretar personopplysningene dine. Legen er underlagt journalplikt og taushetsplikt, og må forholde seg til forskjellige norske lovkrav til hvordan helseopplysninger skal håndteres. Selv om den enkelte av oss neppe kjenner detaljer i lovverket eller helsevesenets datasystemer og informasjonsflyt, vil vi når vi besøker legekontoret forutsette at våre opplysninger blir ivaretatt, og at vi forholder oss til kjente aktører.

Det samme kan ikke sies om personopplysninger innsamlet gjennom apper: Hvilke opplysninger om deg blir lagret, og hvor blir personopplysningene dine av? Er det du som rår over dem eller er det også leverandøren, og muligens også tredjeparter? Hvordan blir dataene sikret?

Dette er informasjon du burde få, enkelt og i en lett forståelig form. Det er med god grunn at informasjon fremstilles som bærebjelken i et godt personvern. Uten slik informasjon kan du ikke ta et bevisst valg. Datatilsynet har derfor sjekket hvilken personverninformasjon du som bruker får hvis du kjøper helserelatert hjemmetestutstyr som er tilgjengelig for en vanlig norsk forbruker.

Testen er Datatilsynets bidrag til årets såkalte GPEN-sveip. GPEN (Global Privacy Enforcement Network) er et nettverk av personvernmyndigheter verden over. Det er fjerde året Datatilsynet deltar i GPEN-sveipet. Årets tema er tingenes internett, gjerne forkortet til IoT (Internet of Things). Vi valgte altså å konsentrere oss om testutstyr for helse. Noen personvernmyndigheter valgte det samme som oss, mens andre valgte for eksempel smart-TVer, smarte biler og leketøy. Totalt 25 personvernmyndigheter verden rundt deltok og så på til sammen 314 objekter.

Hovedinntrykket fra både det norske og det internasjonale sveipet gir grunn til ettertanke: Du kan ikke regne med å få forståelig og dekkende informasjon om bruk av personopplysninger når du kjøper «smarte» produkter som kommuniserer via internett.

Om rapporten

Målet med denne rapporten er å beskrive de viktigste erfaringene vi gjorde under sjekken av helsetestprodukter og tilhørende mobilapper. Vi begrenser oss til å gi en overordnet oppsummering av testen og funnene, og kommer fram til tre konklusjoner.

Totalt sjekket vi personverninformasjon for seks ulike helsetestprodukter. Tallet er lavt. Informasjonen fra vår norske del av GPEN-sveipet er derfor ikke egnet for statistikk og det kan ikke trekkes allmenngyldige konklusjoner. Vår test gir imidlertid et godt innblikk i problematikken for den personvernbevisste forbruker ved bruk av denne type utstyr.

Rapporten er verken ment som, eller kan leses som, en forbrukertest med anbefalinger.

Om testen: Hva og hvordan

Testen handler om personverninformasjon

Testen handler ikke om helsetestutstyret som sådan, men om hvilken *informasjon* om innsamling og bruk av personopplysninger som er tilgjengeliggjort for brukerne. Vi har sett på personvernerklæringen (hvis den var å finne) og informasjon om personvern i andre tekster som i noen tilfeller fantes på appen eller på nettsiden til produsenten.

Testen inneholder ingen teknisk etterprøving av om informasjonen stemmer med hva som faktisk skjer. Testen inneholder heller ikke noen vurdering av om produktenes måleresultater er kvalitativt gode.

Utvalg og innkjøp av produkter

Det finnes et stort utvalg produkter og apper som kan hjelpe deg å gjøre ulike helserelaterte målinger.[1] Gjennom nettsøk og besøk på kjente nettbutikker har vi valgt ut og kjøpt inn testutstyr som norske forbrukere enkelt kan få tak i. I noen grad er det en glidende overgang mellom hva vi kan kalle helse på den ene siden og sunnhet/trening på den andre. Vi ønsket at utstyret i størst mulig grad skulle være tydelig helserelatert, og gjerne aktuelt for personer som har en spesiell sykdom eller lidelse, slik som hjerteproblemer, diabetes eller kols.

Dette valget ble gjort at to grunner. Den ene er å kunne sjekke hvor god personverninformasjonen er når det gjelder måledata som åpenbart er av følsom karakter. Den andre grunnen er at mulig bruk eller overlevering av data fra hjemmetester til fastlege eller helsevesenet er en aktuell debatt. Direktorat for e-helse har for tiden ute på høring et forslag til en selvdeklareringsordning for helse-apper. [2]

Videre har vi valgt å se på testutstyr som er en separat «dings», altså i motsetning til å velge rene apper som utelukkende bruker smarttelefonenes egne sensorer. Det er også mulig å kjøpe elektronisk testutstyr som kun viser/lagrer målingene på selve testutstyret. Hvis opp-lysningene kun lagres på testutstyret har du bedre kontroll på dataene.

Utstyret ble kjøpt fra disse nettbutikkene:

http://www.med24.no

https://test-deg.no

http://www.apple.com/no

http://www.coolstuff.no

http://www.amazon.co.uk

http://www.amazon.com

Siden årets GPEN-tema er Internet of Things (tingenes internett), har kobling mot internett vært en forutsetning. Det gjør testen også mer interessant. At tjenesten bruker internett – gjennom smarttelefonen eller på annen måte – åpner en rekke personvernrelaterte problemstillinger. Behovet for informasjon om bruk av personopplysninger

[1] https://teknologiradet.no/velferd-skole-og-helse/20-mobile-helselosninger-du-kan-ta-i-bruk-na/

[2] https://ehelse.no/horinger/horing-forslag-til-selvdeklareringsordning-for-mobile-helseapplikasjoner

blir mer presserende. Vi har derfor utelukkende kjøpt utstyr som er ment brukt sammen med en smarttelefon.

Vi har testet utstyr som en norsk forbruker enkelt kan bestille fra nettet. For å finne relevant utstyr brukte vi en kombinasjon av rene nettsøk og å se på utvalget hos kjente nettbutikker. Vi endte med å kjøpe utstyr for tre typer testing: Blodtrykk, blodsukker (typisk brukt av diabetikere) og såkalte oksymeter/pulsoksymeter, det vil si måling av oksygenmetning i blodet og puls (aktuelt for kolspasienter).

Vi testet disse apparatene:

- iHealth Wireless Smart Gluco-Monitoring System
- iHealth trådløs Blodtrykksmåler BP5
- iHealth Air Pulse Oximeter
- Withings Blodtrykkmåler Bluetooth
- QardioArm Blood Pressure Monitor
- 2in1 Smart Blodsukkerapparat

Utstyret kostet fra noen hundrelapper til godt over tusenlappen. De tilhørende mobilappene var gratis.

Hvordan testen ble utført

Under testen brukte vi et foreslått skjema fra GPEN (se vedlegg 1) for å kartlegge og vurdere tilgjengelig personverninformasjon sammen med et knippe egne spørsmål (for mer kvalitative observasjoner).

Etter utpakking av utstyr tok vi en rask kikk på bruker-manualer for oppsett og lastet ned nødvendige apper.

Deretter tok vi utstyret i bruk ved å gjennomføre målinger på oss selv. Vi studerte så testresultatene i appen og appens funksjonaliteter. Underveis i prosessen har vi sett etter personverninformasjon – i brukerveiledningen som følger med apparatene, i app-butikken eller i appen selv. Vi har også sett på om produktinformasjon i nettbutikkene vi kjøpte fra oppgir noen personverninformasjon av interesse.

Koblet på mobilen

Sett fra et brukerståsted fungerer alle de seks apparatene i grove trekk likt: Selve apparatet foretar målingen, mens appen som er lastet ned til smarttelefonen viser resultatene. Ett av de seks testapparatene (2in1 Smart Blodsukkerapparat) plugges direkte inn i smarttelefonens utgang for høretelefoner. De øvrige apparatene overfører testresultatene trådløst til smarttelefonen.

I appen kan du typisk se tidligere testresultater fremstilt i grafer, og angivelser at hvilke verdier som er normale, for høye eller for lave, samt annen funksjonalitet. Noen av testapparatene viser også målingstall på selve apparatet.

Testen er ingen dyptgående eller langvarig undersøkelse av hvert enkelt apparat. Den er utført forholdvis raskt, og det kan derfor ikke utelukkes at noe er blitt oversett eller misforstått. Ideen er at vi tar utgangspunkt i en vanlig forbruker som ønsker å orientere seg om hva som skjer med personopplysningene hennes.

Selve testdagene var 11. og 14. april 2016. Testene ble utført av fem av Datatilsynets egne ansatte.

Funn og observasjoner

Hvilken trygghet har forbrukeren for at han eller hun blir godt informert om hvordan deres personvern ivaretas når de bruker testapparatet og den tilhørende appen? Kan en forbruker legge til grunn at han eller hun får dekkende og forståelig informasjon?

Fire av seks mangler personvernerklæring

For hele fire av seks apparater fant vi ingen personvernerklæring. For ett av produktene fant vi ingen personvern-informasjon overhodet– verken i appen, i medfølgende brukerveiledning, eller på selskapets nettside. De andre tre hadde imidlertid noe informasjon om personvern i andre tekster, for eksempel i «Terms of use». Personverninformasjonen for disse tre apparatene gir altså noe enkelt-informasjon av verdi, gitt at brukeren i det hele tatt finner frem til den, men informasjonen oppleves på ingen måte som dekkende.

Varierende kvalitet på informasjon

Den informasjonen som brukeren har tilgjengelig er svært varierende fra produkt til produkt. Resultatene spenner fra ingen informasjon til en del informasjon vi vurderer som relevant og god. Vi fant imidlertid ingen eksempler vi mener er gjennomgående gode og dekkende.

To av produktene hadde personvernerklæring. Her blir det gitt mye relevant informasjon. Dels er teksten god og tydelig på enkelte detaljer. Eksempelvis sier en av personvernerklæringene at data fra europeiske brukere blir lagret på servere i Europa, og at selskapet aldri deler dine data med «advertising platforms, data brokers or information resellers». Deler av tekstene oppleves imidlertid som lite avklarende. Det er også en del spørsmål som blir stående ubesvart, eller fremstår som forvirrende.

Fem av seks får stryk

Personvernerklæring eller ikke - flesteparten av de seks apparatene vi testet hadde altså personverninformasjon i en eller annen grad. Etter å ha vurdert all informasjonen svarte de som sveipet på følgende ja eller nei-spørsmål: «Forklarer personverninformasjonen hvordan personopplysningene blir samlet inn, brukt og delt på en tilfredsstillende måte?». Resultatene er nedslående: Svaret ble nei for fem av testapparatene, og ja for ett av disse. Det tilsvarer 83 prosent nei. De samlede GPEN-tallene viser at 60 prosent av produktene som ble testet internasjonalt ikke hadde tilfredsstillende personverninformasjon.

Vi må imidlertid holde i mente at antallet testobjekter i vårt norske sveipet er lavt, og at hovedinntrykket er sterkt preget av den høye andelen som ikke hadde noen personvernerklæring.

Overordnet viser resultatene fra de seks produktene vi så på at en forbruker *vanskelig* kan ha trygghet for at han eller hun blir godt informert om hvordan personvernet blir ivaretatt. Kjøperen kan ikke belage seg på at forståelig og dekkende informasjon er enkelt tilgjengelig. Dette er både noe uventet og skuffende, særlig tatt i betraktning av at vi har sett på utstyr som samler inn data som gir indikasjoner på din helsetilstand.

Hvor er dataene lagret og hvem har råderetten?

Vi vil trekke frem to forhold som vi særlig mener at brukeren burde få informasjon om: Hvor er dataene lagret og hvem har råderetten over disse?

Når det brukes et separat testapparat og en smarttelefon, kan dataene befinne seg flere steder:

- I selve testapparatet (eksempelvis at apparatet lagrer de siste 100 målingene).
- I smarttelefonen
- På servere/i skyen
- Delt med tredjeparter

Ingen av produktene vi så på forklarte på en god måte hvordan og hvor personopplysningene blir lagret. Brukerne ble heller ikke gitt valgmulighet med hensyn til hvor dataene skulle lagres. For eksempel om dataene kun skal lagres i produktet selv eller i «skyen».

Noen av apparatene hadde eksplisitt informasjonen om at et antall avlesninger ble lagret i selve testapparatet. For de andre apparatene vet vi ikke hva som er realiteten. Hva skjer hvis du gir eller selger apparatet til andre? Får ny eier tilgang til dine data i testapparatet? Ingen av apparatene hadde informasjon om, og i så fall hvordan, data på testapparatet kunne slettes.

Med hensyn til råderett over dataene, altså hvem det er som kan bestemme over personopplysningene, fant vi ofte informasjon som ikke gav klare nok svar. I noen grad opplevde vi også beskrivelsene som motstridende. For eksempel oppga en leverandør at brukeren hadde full kontroll over egne opplysninger, men senere i teksten står det at leverandøren kan bruke opplysningene i visse tilfeller.

Oppsummering av resultatene for det enkelte produkt i det norske sveipet

	Withings Blodtrykk-måler Bluetooth	QardioArm Blood Pressure Monitor	2in1 Smart Blodsukker-apparat	iHealth Wireless Smart Gluco-Monitoring System	iHealth trådløs Blodtrykks-måler BP5	iHealth Air Pulse Oximeter
Personvern-erklæring	✓	✓	✗	✗	✗	✗
Informasjon om hvordan opplysninger blir brukt	✗	✓	✗	✗	✗	✗
Informasjon om lagring og sikkerhet	✗	✗	✗	✗	✗	✗
Kontaktinfor-masjon om personvern-spørsmål	✓	✓	✗	✗	✗	✗
Informasjon om sletting	✗	✗	✗	✗	✗	✗

Tre konklusjoner

Brukervennlig utstyr, men ikke brukervennlig informasjon

Vår generelle erfaring fra sveipet er at utstyret er svært brukervennlig. Det er enkelt å komme i gang, installere mobilappene og å få det hele til å virke, ta tester og å lese av resultater. Det er derfor noe paradoksalt i at det ofte er så *vanskelig* for brukeren å finne dekkende informasjon om hvordan personopplysningene som registreres blir håndtert.

Behovet for lett tilgjengelig informasjon har vært påpekt av personvernaktører over lang tid. Vårt inntrykk er at personvernerklæringer eller liknende har blitt betydelig mer utbredt med tiden. At fire av seks produkter i vår test ikke har personvernerklæring, viser imidlertid at slike erklæringer fremdeles ikke er en selvfølge - selv fra seriøse aktører (noe vi oppfatter selskapene bak apparatene som). Det er en situasjon man ikke lett kan slå seg til ro med.

Personvern-erklæring er viktig!

Datatilsynet anbefaler alle virksomheter som behandler personopplysninger å utarbeide en egen personvernerklæring når det skal informeres om virksomhetens bruk av personopplysninger. Dersom personverninformasjonen spres i andre tekster, vil det lett blir vanskelig å se helheten, og sannsynligheten er stor for og at viktige punkter ikke er kommentert. Du finner veiledning om personvernerklæringer på datatilsynet.no

Kjøp først, ta stilling senere?

Selvråderett er et viktig prinsipp for godt personvern, og informasjon er en forutsetning for at den enkelte av oss kan ta bevisste valg: Ønsker du å ta i bruk dette produktet eller tjenesten eller ikke? Finnes det kanskje andre produkter som ivaretar ditt personvern på en bedre måte? Informasjon er ikke bare nødvendig – det har også betydning *når* informasjonen kommer. Informasjonen må komme *før* man tar utstyret i bruk – og selvsagt aller helst også før man kjøper det.

I vår test har vi ikke sett eksempler på at nettbutikken gir personverninformasjon eller linker til personvern-erklæringer eller liknende. Oftest sies det ikke engang navnet på den appen som apparatet bruker (det går frem av brukerveiledningen som følger med i pakken). Appens navn kunne i det minste gjort det lettere for forbrukeren å undersøke videre i app-butikken før man går til det skritt å kjøpe produktet. App-butikkens beskrivelse har gjerne peker til personvernerklæring. For Android vil det her også fremgå hvilke tilganger appen krever på din smarttelefon.

Testen viste oss at den personvernbevisste forbrukeren har en særlig utfordring med hensyn til kombinasjonen av separate testapparater og mobilapper: Mest sannsynlig har forbrukeren allerede kjøpt og betalt utstyret før han eller hun får personverninformasjon av verdi.

Forbrukere som ønsker å ta et informert valg (med henblikk på eget personvern) må altså selv lete i app-butikken og på produsentenes nettsider, i håp om å finne riktig informasjon.

Datasikkerhet

Alle appene hadde mulighet for videreformidling av testresultater. En av appene hadde også mulighet for å dele testresultater på Twitter og Facebook direkte fra appen.

Alle appene hadde mulighet for å sende resultater per e-post. Vi legger her til grunn at dette er alminnelig ukryptert e-post. I praksis kunne det legges inn en hvilken som helst e-postadresse (venner, familie eller hvem som helst). Tjenestene var imidlertid, som hovedregel, penset inn på kontakt med helsevesenet.

Flere av appene legger opp til deling med helsetjenesten

Denne funksjonaliteten gir grunn til ettertanke. Det gjelder med hensyn til brukernes kunnskaper og mulighet for å beskytte seg selv. Det gjelder også i relasjon til kravene i norsk regelverk.

Å sende sensitive personopplysninger (helsedata inkludert) per e-post er som hovedregel ikke tillatt. Informasjonssikkerhetsbestemmelsene i personvern-regelverket krever en tilfredsstillende sikring av personopplysninger, og vanlig e-post regnes som for lite sikkert for personopplysninger med høyt beskyttelsesnivå. Regelverket gjelder imidlertid ikke for enkeltmenneskers bruk av personopplysninger for private formål. Reglene gjelder for virksomheter, for eksempel et legekontor.

Helseaktørers, for eksempel fastlegers, bruk av pasienters data fra hjemmetesting er en aktuell debatt. Hvis helseaktører skal motta denne type data fra pasientene, er vanlig e-post en klart utilfredsstillende løsning. Pasientenes sensitive personopplysninger blir ikke tilfredsstillende beskyttet.

Personvern handler om få velge selv, og å kunne ta bevisste valg. Ønsker en enkeltperson å publisere sine blodtrykksmålinger på internett, er det en frihet vedkommende har. Det er imidlertid viktig at profesjonelle aktører bidrar til at personer forstår konsekvensene av, og risikoen ved, ulike valg.

Funn fra det internasjonale sveipet

25 tilsynsmyndigheter fra hele verden sveipet til sammen 314 produkter. I tillegg til hjemmetester innen helse ble blant annet «fitness wearables», «smart meters», smart-TVer og smarte husholdningsartikler sveipet.

- 59 prosent av produktene som ble testet informerte ikke brukerne om hvordan personopplysninger blir samlet, brukt og delt på en god måte.
- Produktene i det internasjonale sveipet samlet inn følgende informasjon fra brukeren:
    - Navn – 84 prosent av produktene
    - E-post – 83 prosent av produktene
    - Fødselsdato eller alder – 64 prosent av produktene
    - Lokasjon – 68 prosent av produktene
    - Adresse – 53 prosent av produktene
    - Telefonnummer – 55 prosent av produktene
    - Bilder/video/audio – 41 prosent av produktene
    - UDI (Unique Device Identifier) – 61 prosent av produktene
- 38 prosent av produktene oppgav ikke kontaktinformasjon slik at brukerne enkelt kan henvende seg hvis de har spørsmål rundt personvern.
- 68 prosent av produktene i testen forklarte ikke hvordan personopplysninger blir lagret. Bare halvparten av produktene informerte om hvilke sikkerhetstiltak leverandøren tar for å sikre personopplysningene til brukeren (passordbeskyttelse, autentisering ved innlogging osv).
- 72 prosent av produktene i testen gav ikke brukeren tilfredsstillende informasjon om hvordan brukeren kan gå fram for å slette personopplysningene sine.

VEDLEGG: GPEN sveipeskjema

GPEN Sweep 2016 – example Sweep form

Basic info Device type	Wearable ☐ Health-related device ☐ Smart TV ☐ Appliance ☐ Smart meter ☐ Connected car ☐ Other ☐ Please state													
Device/company details	Device name:	Name of organisation:	Sector:	Relationship of org to device:	Country of relevant company:									
Collection, use & disclosure of data	Does the website/app have a privacy policy? ☐Y ☐N Do privacy communications indicate what personal information is collected by the device? ☐Y ☐N Are privacy communications specific to the device? ☐Y ☐N Do privacy communications state that personal information is disclosed to other companies and for what purpose? ☐Y ☐N ☐Don't know If the company does share information with other companies, is the user told *which* companies? ☐Y ☐N ☐N/A Are users told to change the default settings for the device? ☐Y ☐N How do users consent to the collection of their personal data? ☐ Through literature ☐ On the device itself ☐ During registration ☐ Other ..... ☐ Don't know													
Information collected **M**andatory **O**ptional **N**ot **C**ollected	**During registration**									**During use**				
	Name	User name	Address	Phone number	Email address	DOB/ age	Weight / height	Medical details (e.g. diabetic)	Other (please state)	Location	Health/ Fitness info (e.g. heartrate)	Photo/ Video/ Audio file	Unique device ID	Other (please state)
	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC	☐M ☐O ☐NC
Explanation for how info is used?	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N	☐Y ☐N
Storage of information and safeguards	Do privacy communications make reference to the *storage* of personal information collected by the device? ☐Y ☐N Is personal information stored and/or transferred in an *encrypted* form? ☐Y ☐N ☐Don't know Do privacy communications mention the use of security safeguards to keep unauthorised users from accessing the device or data? (e.g. password protections or authentication questions?) ☐Y ☐N Is the data stored in the same country as the manufacturer/relevant data controller? ☐Y ☐N ☐Don't know Does the company use third parties to store data? ☐Y ☐N ☐Don't know (***If company is contacted directly***) Did the company conduct any risk assessment procedures to identify potential privacy risks associated with the device? ☐Y ☐N ☐Don't know													

Contact information	Do privacy communications include contact details to allow a user to contact the company about privacy related matters? ☐ Y ☐N				
Deleting personal information	How many steps are required to delete personal information from the device? ..... Are deletion instructions clear and easy to follow? ☐Y ☐N ☐N/A If a user sells their device, does the company provide tools to help clear the device of personal data? ☐Y ☐N ☐Don't know If a user loses their device, are tools available to delete/remove personal data from the device (i.e. remote wiping)? ☐Y ☐N ☐Don't know				
OPTIONAL DC response	Did the data controller respond within the deadline? ☐Y ☐N Did the response address all questions? ☐Y ☐N Was the response clear and easy to understand? ☐Y ☐N				
INDICATOR Based on the above responses	1) Do privacy communications adequately explain how PI is **collected, used** and **disclosed**?	2) Are users fully informed about how personal information collected by the device is **stored** and are there **safeguards** to prevent loss of data?	3) Do privacy communications include **contact details** for individuals wanting to contact the company about a privacy-related matter?	4) Do privacy communications explain how a user can **delete** their information?	5) Did the data controller provide a **timely, adequate** and **clear** response?
RESPONSE Answer: Y or N (see advice below)					
Comments: Any positive observations identified during the Sweep (in relation to the communication of privacy information to customers) – whether related to the questions or not.			Any additional concerns identified during the Sweep – whether related to the questions or not.		

Besøksadresse:
Tollbugata 3, 0152 Oslo

Postadresse:
Postboks 8177 Dep.,
0034 Oslo

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no