Datatilsynet

PepCall AS
Munkedamsveien 35

0250 Oslo

Deres referanse	Vår referanse	Dato
	17/01484-14/EOL	20.12.2017

Vedtak om pålegg - PepCall AS - Personvern og informasjonssikkerhet i smartklokker

Vi viser til vårt varsel om vedtak av 7. desember 2017 samt korrigert versjon av 12. desember 2017. Vi mottok deres merknader til varselet innen fristen den 15. desember 2017. Vi hadde dessuten noen oppfølgingsspørsmål som vi avklarte fortløpende i etterfølgende e-postkorrespondanse. Våre kommentarer til merknadene følger under.

Vedtak om pålegg
Datatilsynet vedtar følgende pålegg:

1. PepCall AS må stoppe all behandling av personopplysninger som er i strid med personopplysningsloven § 14. PepCall AS har ikke etablert og vedlikeholdt de planlagte og systematiske tiltak som er nødvendige for å oppfylle grunnleggende plikter etter personopplysningsloven.

2. PepCall AS må stoppe all behandling av personopplysninger som er i strid med personopplysningsloven § 13. PepCall AS har ikke sørget for tilfredsstillende informasjonssikkerhet med hensyn til vern av konfidensialitet og integritet for kunders personopplysninger lagret ved bruk av Xplora med tilknyttet app.

3. PepCall AS må informere sine kunder om sikkerhetshullene som har foreligget og sikkerhetshullene som fortsatt foreligger. Dette er informasjon kundene har krav på i medhold av personopplysningsloven § 19 første ledd bokstav c.

   PepCall AS må også forklare sine kunder den risiko som sikkerhetshullene innebærer for kompromittering av personopplysninger. Informasjonen må være i en lett forståelig form.

Vår hjemmel for å fatte pålegg om at lovstridig behandling av personopplysninger skal opphøre er personopplysningsloven § 46 fjerde ledd.

Fristen for å gjennomføre påleggene er **15. januar 2018.** Innen denne fristen må dere sende oss en skriftlig bekreftelse på at påleggene er gjennomført.

Nærmere om sakens faktiske forhold
PepCall AS er behandlingsansvarlig og markedsfører av smartklokken Xplora med tilknyttet app på det norske markedet. Smartklokker er beregnet for barn og som har det meste av funksjonalitet tilsvarende en mobiltelefon. Foresatte kan via en applikasjon holde kontakt med barnet og samtidig ha oversikt over barnets lokasjon.

Forbrukerrådet gjorde tidligere i høst en undersøkelse av sikkerheten i ulike typer smartklokker tilgjengelige på det norske markedet. En av klokkene som ble undersøkt var Xplora. Det ble gjort funn som for eksempel at det var mulig for uvedkommende å få tilgang til beskyttelsesverdige personopplysninger om brukere lagret på Xploras servere (inklusive navn, telefonnummer, lokasjonsdata og kontaktinformasjon). Det var også mulig å få tilgang til informasjon fra andre brukere.

På bakgrunn av Forbrukerrådets undersøkelser og funn rettet Datatilsynet en henvendelse til PepCall AS med krav om redegjørelse for en rekke forhold knyttet til etterlevelse av personopplysningsloven. Datatilsynets krav om redegjørelse var ikke kun knyttet til de spesifikke produktene som Forbrukerrådet hadde undersøkt eller kun informasjonssikkerheten, men en bredere kontroll av hvordan PepCall AS ivaretar kundenes personvern og sørger for tilfredsstillende informasjonssikkerhet for alle tilsvarende produkter som virksomheten tilbyr på markedet.

Etter gjennomgang av PepCall AS sitt tilsvar til Datatilsynets krav om redegjørelse sendte vi et varsel om vedtak med frist for å komme med merknader før eventuelt vedtak fattes. Etter gjennomgang av PepCall ASs merknader har vi kommet til at vi opprettholder vårt varslede vedtak. I det følgende vil vi gjennomgå grunnlagene for vårt vedtak, PepCall AS sine merknader og våre konklusjoner.

Informasjonssikkerhet
Etter personopplysningsloven § 13 skal den behandlingsansvarlige gjennom systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet. Personopplysningsforskriften kapittel 2 inneholder mer detaljer med hensyn til hva plikten til å ivareta informasjonssikkerhet innebærer.

Plikten til å ivareta informasjonssikkerhet innebærer blant annet at behandlingsansvarlig skal sørge for forholdsmessig sikring av personopplysninger, jf. personopplysningsloven § 13, jf. personopplysningsforskriften § 2-1. Der behandling av personopplysninger innebærer en risiko for liv og helse, økonomisk tap eller tap av anseelse og personlig integritet skal planlagte og systematiske tiltak treffes for å ivareta informasjonssikkerheten.

Det følger av personopplysningsloven § 15 at en databehandler ikke kan behandle eller overføre opplysninger til en tredjepart uten at dette er skriftlig avtalt med den behandlingsansvarlige. Ansvaret for avtaleinngåelsen kan gjerne delegeres, men behandlingsansvaret og pliktene som følger av dette kan ikke delegeres.

Dette betyr at dere har ansvaret for å beslutte hvorvidt tjenesteutsetting i stort omfang er forsvarlig. Det innebærer ansvar for om personvern blir ivaretatt, at det foreligger tilstrekkelig informasjonssikkerhet og en aksept av restrisiko. Det kan ikke delegeres til andre, som for eksempel databehandlere eller andre konsulenter.

Styring og kontroll er nødvendig for å sikre at den behandlingsansvarlige etterlever sine lovpålagte plikter til blant annet å vurdere risiko og personvernkonsekvenser ved tjenesteutsetting av IKT-drift og infrastruktur jf. personopplysningsloven § 15 og personopplysningsforskriften kapittel 2. Ledelsens plikt til å ha kontroll med virksomhetens informasjonssikkerhet kommer også klart til uttrykk i personopplysningsforskriften § 2-7. Bestemmelsen fastsetter krav om klare ansvars- og myndighetsforhold for bruk av informasjonssystemet. Det stilles også krav om at endringer av konfigurasjon skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglig leder.

Den behandling av personopplysninger som foretas ved bruk av smartklokkene til PepCall AS er i aller høyeste grad egnet til å innebære en risiko for liv og helse, økonomisk tap eller tap av anseelse og personlig integritet. Klokkene med tilhørende app genererer opplysninger som kommunikasjon (til, fra, innhold, logg, SMS) og lokasjon. Sikkerhetsavvikene som ble avdekket av Forbrukerrådet i samarbeid med mnemonic synliggjorde hva risikoen består i. mnemonic avdekket at uvedkommende kunne få tilgang til beskyttelsesverdige personopplysninger om brukere av Xplora-klokkene. Barn er en sårbar gruppe og virksomheter som behandler personopplysninger om barn er forpliktet til å ha en særskilt aktsomhet hva gjelder forhold av betydning for barns personvern. Dette tilsier at informasjonssikkerheten skal være høyt prioritert og på et høyt nivå.

De sikkerhetshull som ble avdekket av Forbrukerrådet i samarbeid med mnemonic var graverende. Det ble blant annet avdekket at det har vært mulig for uvedkommende å få ut beskyttelsesverdige personopplysninger om brukere lagret på Xploras servere (inklusive navn, telefonnummer, lokasjonsdata og kontaktinformasjon). Det var også mulig å få tilgang til informasjon fra andre brukere. I følge personopplysningsforskriften § 2-14 har PepCall AS en eksplisitt plikt til å iverksette tiltak for å oppdage slik bruk.

Personopplysningsforskriften §§ 2-11 fastslår videre virksomhetens plikt til å sørge for opplysningenes konfidensialitet. Det at personopplysninger har vært tilgjengelige for uvedkommende er et brudd på denne plikten.

De første svarene vi mottok fra PepCall AS inneholdt ingen dokumentasjon som tydet på at ledelsen i PepCall AS hadde vurdert og tatt stilling til i hvilken grad restrisiko er akseptabel for sin virksomhet. I sitt svarbrev sendt 10. november 2017 informerer PepCall AS om at det ikke er foretatt risikovurderinger, annet enn at det under utvikling ble foretatt valg for å begrense tilgangen til personopplysninger (lokasjonsdata), men at databehandler Infomark var i ferd med å gjøre dette. Det ble den 24. november 2017 ettersendt en risikovurdering gjennomført av Infomark. PepCall AS har videre sammen med tjenesteeier Xplora Technologies Ltd. inngått avtale med et konsulentselskap (TÜVIT) som skal sørge for at informasjonssikkerheten blir ivaretatt for klokkene med tilknyttet applikasjon.

Etter vårt varsel om vedtak har vi fått tilsendt noe dokumentasjon knyttet til risikovurdering. Etter gjennomgang av denne mener vi fortsatt at det mangler en helhetlig tankegang knyttet til vurdering av risiko ved behandling av personopplysninger. Sentrale elementer i risikovurdering som f.eks vurdering av sannsynlighet (hvor lett kan risikoscenariene skje), beskrivelser av konsekvens, trusler og sårbarheter mangler.

Vi mener også at det mangler relevante scenarier som gjør det mulig å gjøre en reell vurdering av konfidensialitet, integritet og tilgjengelighet for den tjenesten som tilbys. Med de sikkerhetshull som er blitt avdekket som bakteppe hadde vi forventet å finne scenarier som for eksempel beskriver uautorisert tilgang eller endring av personopplysninger, uautorisert og utilsiktet utlevering eller endring av personopplysninger, tilgang fra ikke-brukere, ansatte, administratorer, etc.

Vi hadde også forventet å finne beskrivelser av tiltak som er egnet til å forebygge/hindre de risikoer som blir identifisert. PepCall AS har beskrevet noen tiltak ved sikkerhetshendelser, men samtlige går ut på å gjøre noe i etterkant av at hendelsen har skjedd.

Det er positivt at PepCall AS har startet på en prosess for å få utarbeidet risikovurderinger og at det er inngått avtaler med virksomheter med kompetanse på revisjon og sikkerhetstesting. Vi registrerer imidlertid at den risikovurderingen vi først fikk oversendt var av henholdsvis de to sårbarhetene som mnemonic påviste. PepCall AS hadde altså ikke gjort noen egen risikovurdering basert på egen interkontroll og oversikt over personopplysninger, verdivurdering og trusler. Risikovurderingen vi mottok i siste brev er etter Datatilsynets mening for mangelfull til å være et forsvarlig beslutningsgrunnlag.

Vi etterlyser en mer helhetlig tankegang knyttet til vurdering av risiko ved behandling av personopplysninger. PepCall AS legger for eksempel stor vekt på at personopplysninger kun lagres innen EU (Irland og Tyskland), mens det i rapporten fra Infomark fremgår at Infomark IT department hoster applikasjonen, noe som betyr at de også har tilgang til personopplysningene som behandles i appen. Dette er også bekreftet av PepCall AS i etterfølgende e-post korrespondanse. PepCall AS argumenterer i sitt svar for at tilgang til personopplysninger ikke er en behandling av personopplysninger, og viser i den forbindelse til definisjonen av «behandling» personopplysningsloven § 2 nr 2.

Begrepet «behandling» i personopplysningsloven er svært vidt, og omfatter som ordlyden sier «enhver bruk av personopplysninger». Listen over måter å behandle personopplysninger som følger er ikke uttømmende – noe som understrekes ved at det står «for eksempel» foran opplistingen.

Personopplysningsloven er ment å gjennomføre personverndirektivet (directive 95/46/EC) i norsk rett. I personverndirektivets definisjon av behandling går det enda tydeligere frem at begrepet skal tolkes svært vidt. I art. 2 bokstav b står det at en «behandling av personopplysninger er:

«enhver operasjon eller rekke av operasjoner som med eller uten elektroniske hjelpemidler utøves i forbindelse med personopplysninger, for eksempel innsamling, registrering,

systematisering, oppbevaring, tilpasning eller endring, gjenfinning, søking, bruk, videreformidling ved overføring, spredning eller andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, sperring, sletting eller tilintetgjøring».

I likhet med ordlyden i personopplysningsloven går det tydelig frem at opplistingen ikke er uttømmende. I tillegg er «tilgjengeliggjøring» nevnt spesifikt – noe som etter en naturlig ordlydsfortolking vil inkludere tilgang til opplysninger via en digital plattform.

Argumentasjonen over viser at for vurderingen av om noe omfattes av begrepet «behandling» i personvernregelverket er det ikke avgjørende at den som har tilgang til opplysningene faktisk foretar seg noe med dem (prosesserer). Tilgang til personopplysninger i seg selv en behandling. Når personopplysninger er tilgjengelige for ansatte i Infomark i Sør-Korea så er dette pr definisjon en behandling av personopplysninger. Behandlingen skulle vært informert spesifikt om til kundene, det må inngås databehandleravtale med Infomark, og en standardavtale for overføring til tredjeland.

I varsel om vedtak stilte vi spørsmål ved om PepCall AS har oversikt over det totale økosystemet for utvikling og drift av klokker, apper og servere, og om de har kontroll med hvilke personopplysninger som genereres, sendes og lagres hvor. Spesielt ble det trukket frem at det i rapporten fra Infomark fremgikk bruk av to virksomheter som ikke var nevnt som samarbeidsparter av PepCall AS (LinkMobility.com og Unwiredlabs.com). Disse virksomhetene har PepCall AS i sitt siste brev gjort rede for, og det er vårt inntrykk at de har kontroll på disse og flyten av data som administreres av disse.

Som behandlingsansvarlig skal PepCall AS være i forkant og iverksette planlagte og systematiske tiltak for å ivareta informasjonssikkerheten. Det er ikke tilstrekkelig å lukke avvik etterhvert som de blir påvist av andre. Det er heller ikke tilstrekkelig å kun basere seg på en risikovurdering gjort av en databehandler eller en risikovurdering som ikke gir tilstrekkelig beslutningsgrunnlag.

Som behandlingsansvarlig skulle PepCall AS ha gjennomført risikovurderinger før behandling av personopplysninger iverksettes og før informasjonssystemet tas i bruk. Risikovurderinger skal også gjennomføres ved endringer i forhold som kan påvirke informasjonssikkerheten, for eksempel endringer i behandlingen eller endringer i trusselbildet.

Vi ser at det er gjort noen risikovurderinger i forbindelse med valg av tjenesteleverandører. Vi kan imidlertid ikke se at disse er oppdatert eller en del av en systematikk/syklus som gjør det mulig å håndtere ny sikkerhetsrisiko. Etter Datatilsynets oppfatning har ikke PepCall AS demonstrert planlagte og systematiske tiltak som er egnet til å håndtere den sikkerhetsrisiko som produktene deres innebærer for behandling av personopplysninger.

Vår vurdering er at PepCall AS i etterkant av denne kontrollsaken har iverksatt tiltak for å ta eierskap til, og kontroll med behandling av personopplysninger i sine produkter og informasjonssystem. Vi viser til opprinnelig redegjørelse der det fremgikk at det var Infomark som var ansvarlige for risikovurderinger. For de som var kunder før denne saken kom opp betyr det at de fikk liten eller ingen informasjon om hvor deres personopplysninger var

tilgjengelige og at PepCall AS i stor grad overlot ansvaret for beslutninger som har betydning for kundenes personvern og informasjonssikkerheten knyttet til behandling av personopplysninger, til databehandler og konsulenter.

PepCall AS mener at den oversendte dokumentasjonene viser at det er de som behandlingsansvarlig som har oversikt og som tar avgjørelsene knyttet til personvern og informasjonssikkerhet. Vi ser at det er gjort forbedringer ved at PepCall AS blant annet har igangsatt utarbeidelse av risikovurdering, inngåelse av avtaler med databehandlere og kontroll med underleverandører. Som påpekt ovenfor mener vi imidlertid at risikovurderingene er mangelfulle og at de som var kunder før denne saken kom opp ikke har fått sine rettigheter etter personvernregelverket oppfylt. Vi mener det er alvorlig at PepCall AS har valgt å definere «behandling» av personopplysninger så innskrenkende at tilgang til personopplysninger fra databehandles underleverandør ikke vurderes som en behandling. Vi mener for det første at regelverket er tydelig på at behandlingsbegrepet er svært vidt, og at PepCalls tolking ikke er forsvarlig. For det andre er dette en tolking som kan få store konsekvenser for risikovurderingene som virksomheten gjør.

På bakgrunn av redegjørelsen ovenfor fastholder Datatilsynet at sakens opplysninger underbygger at måten sikkerhetsarbeidet er organisert så pulveriserer det ansvaret for å sikre at den behandlingsansvarliges plikter etterleves. Konsekvensen av dette er manglende forankring og kontroll med beslutninger som tas.

Konklusjon
Manglende kontroll og manglende rutiner for å sikre kontroll anses å være i strid med kravene i personopplysningsloven §§ 13-15 og personopplysningsforskriften §§ 2-3 og 2-7.

Informasjon til kundene
Personopplysningsloven §§ 18 og 19 oppstiller særskilte informasjonsplikter overfor de som det behandles personopplysninger om. Informasjonen skal gis i forkant av at opplysningene innhentes og være tilpasset den konkrete behandlingssituasjonen.

Personopplysningsloven § 19 første ledd bokstav c fastslår at den behandlingsansvarlige skal informere den registrerte om opplysningene vil bli utlevert. Datatilsynet har lagt til grunn at denne bestemmelsen innebærer at behandlingsansvarlig skal informere registrerte når personopplysninger blir utlevert som følge av sikkerhetsavvik. Denne fortolkingen er stadfestet av Personvernnemnda.

På det tidspunkt hvor Datatilsynet ba om redegjørelse fra PepCall AS forelå det ingen informasjon tilgjengelig om hvordan PepCall AS behandler personopplysninger ved kunders bruk av deres produkter. Etter vårt krav om redegjørelse var det fremdeles ingen informasjon på PepCall AS.no, men på Xplora.no, Appstore og GooglePlay ble det publisert en personvernerklæring. I varsel om vedtak fremholdt Datatilsynet at den informasjonen som ble gitt i personvernerklæringen, og formen den ble gitt i, ikke tilfredsstiller kravene i personopplysningsloven §§ 18 og 19.

Bakgrunnen for dette er at det i denne saken for eksempel er vanskelig å få oversikt over ansvarsforhold og relasjoner mellom ulike virksomheter (behandlingsansvarlige, databehandlere, leverandører, teleoperatører, etc). Oversikt og informasjon om hvem som har ansvar for hva og hvor personopplysninger utveksles mener vi er grunnleggende for at de registrerte skal kunne ta et informert valg, og slik informasjon inneholdt personvernerklæringen ikke. Det fremgikk heller ingen informasjon om hvilke personopplysninger som behandles, hvilke opplysninger som er nødvendige å behandle for at tjenesten skal fungere og hvilke personopplysninger som man frivillig (samtykke) kan oppgi for å få tilgang til ekstra funksjonalitet, ingenting om at personopplysninger er tilgjengelig for databehandler i Sør-Korea.

I tillegg til å være mangelfull mener vi at informasjonen i PepCall AS sin opprinnelige personvernerklæring var lite tilgjengelig. I en personvernerklæring forventer vi å finne informasjon relatert til hvordan leverandøren av appen forholder seg til europeisk personvernregelverk (siden appen markedsføres mot norske kunder) i en lett forståelig form. Det dokumentet vi fant var forfattet på engelsk og skrevet med et juridisk, komplisert språk. Dette gjør det svært vanskelig for kunden å forstå hvordan personopplysningene faktisk blir brukt. Etter vår vurdering vil det å ha en personvernerklæring på engelsk medføre at svært mange ikke vil kunne sette seg tilstrekkelig inn i hvilken personvernpolicy virksomheten har. Dette gjør seg spesielt gjeldende hvor ansvarsforholdene er uoversiktlige slik som det er tilfelle med smartklokkene.

Det er vanskelig for brukerne av appen å forutberegne sin rettsstilling fordi varierende grad av engelskkunnskaper gjør at det reelle meningsinnholdet i ord og uttrykk ikke nødvendigvis vil være forståelig. Etter vår vurdering kan reell forståelse kun sikres ved at retningslinjer for personvern skrives på norsk når tjenesten henvender seg til norske brukere.

PepCall AS er ikke enige med Datatilsynet i at informasjonen som ble gitt i personvernerklæringen var mangelfull eller villedende, og heller ikke at den var lite tilgjengelig. Dere fremholder at grunnen til at det er mye om komplisert tekst er at kravene i personvernforordningen tilsier et slikt presisjonsnivå.

Til tross for uenigheten har PepCall AS utarbeidet en forenklet personvernerklæring på norsk. Denne inneholder etter vår vurdering tilstrekkelig informasjon i en lett forståelig form med hensyn til både språk og formuleringer.

Ved nedlasting av app i Appstore og GooglePlay er imidlertid informasjonen fremdeles kun på engelsk. Vi viser til argumentasjonen over for hvorfor vi mener at også denne må være tilgjengelig på norsk.

Det er positivt at PepCall AS har utarbeidet ny og bedre informasjon til sine kunder om hvordan de behandler personopplysninger. Når det gjelder informasjonens eventuelle betydning for valget av å ta i bruk tjenesten vil den nye informasjonen kun ha virkning for nye kunder. Kunder som har kjøpt klokker før november 2017 ikke har fått noen informasjon, mens kunder som har kjøpt klokker i november/desember 2017 har fått mangelfull og villedende informasjon, jf informasjonen over.

Datatilsynet har i varsel om vedtak lagt til grunn at ingen kunder har fått informasjon om de sikkerhetsavvik som har forekommet, og har følgelig ikke fått mulighet til å innrette seg etter at beskyttelsesverdig informasjon knyttet til deres barn kan være på avveier. PepCall AS mener at kundene ble informert i form av en e-post som ble sendt ut i oktober 2017 som omtaler Forbrukerrådets rapport om sikkerhetshull i smartklokker i generelle former. Til tross for at PepCall AS mener at de har oppfylt informasjonsplikten overfor kundene så vil det på bakgrunn av Datatilsynets vurdering av det motsatte bli sendt ut ytterligere informasjon. Datatilsynet har fått tilsendt utkast til ny informasjon i to omganger.

Etter Datatilsynets vurdering underkommuniserer PepCall AS egen roll/skyld i manglende etterlevelse av regler som gjelder for personvern og informasjonssikkerhet. Dette gjelder både den tidligere informasjonen og første utkast til ny tekst. Teksten fremstår mer som et virkemiddel for å sette PepCall AS i et bedre lys enn konkurrentene enn en informasjon til kundene om faktiske sikkerhetsavvik som kan ha hatt konsekvenser. Kundene deres må få klar og tydelig informasjon om hva PepCall AS sin manglende etterlevelse av regelverket består i. I svarbrevet vektlegger dere at dere ikke har indikasjoner på at personopplysninger er på avveier, men realiteten er at dette ikke kan fastslås med sikkerhet. Poenget med informasjonen er at deres kunder skal kunne innrette seg etter det som har skjedd og for eksempel ta egne forholdsregler med hensyn til risikoen for at personopplysninger kan være på avveier.

I første utkast var det også en referanse til at PepCall AS har initiert et samarbeid med Datatilsynet knyttet til sikkerhet i smartklokker. Dette mener vi er direkte misvisende og må fjernes. Som det går frem av korrespondansen så sendte PepCall AS riktignok en e-post til Bjørn Erik Thon tidligere i år, men e-posten ble ikke besvart og det ble heller ikke igangsatt noe samarbeid eller dialog. Det er villedende å gi inntrykk av at det eksisterer et slikt samarbeid når det i realiteten ikke har vært kontakt før denne kontrollsaken ble igangsatt.

I andre utkast av informasjon har PepCall AS tatt inn konkret informasjon om hva deres sikkerhetsavvik besto av, hvilke personopplysninger som ble eksponert og innrømmelse av at personvernerklæringen har vært lite tilgjengelig. I tillegg er referansen til samarbeid med Datatilsynet fjernet. Dette er etter vår vurdering en tilfredsstillende korrigering av informasjon.

PepCall AS har gjort gode utbedringer av den informasjonen som blir gitt kunder fremover. Nytt informasjonsskriv om sikkerhetshullene er tilfredsstillende og forutsatt at personvernerklæring ved nedlasting av app i Appstore og GooglePlay gjøres tilgjengelig på norsk vil informasjonsplikten for fremtidige kunder være oppfylt.

Det er imidlertid fortsatt mangler som tilsier at informasjonsplikten i personopplysningsloven §§ 18 og 19 ikke er oppfylt. Det faktum at PepCall AS har foretatt en innskrenkende tolkning av begrepet «behandling av personopplysninger» medfører for eksempel at kundene ikke får informasjon om alle som har tilgang til deres personopplysninger. På bakgrunn av ovennevnte mener Datatilsynet at informasjonsplikten ovenfor kundene ikke er overholdt og at særlig kunder som har kjøpt smartklokker fra PepCall AS inntil desember 2017 ikke har vært gjort i stand til å gjøre informerte valg fordi informasjonen inntil nylig har vært mangelfull.

Konklusjon
Manglende og villedende informasjon til de registrerte er i strid med kravene i personopplysningsloven §§ 18 og 19, og § 14, jf. personopplysningsforskriften § 3-1.

Internkontroll
Personopplysningsloven § 14 fastslår at behandlingsansvarlige skal etablere og holde ved like planlagte og systematiske tiltak som er nødvendige for å oppfylle krav og plikter etter personopplysningsloven. Personopplysningsforskriften kapittel 3 inneholder mer detaljer med hensyn til hva plikten til å ha internkontroll innebærer.

I vårt brev av 16. oktober 2017 ba vi om redegjørelse for en del sentrale elementer i internkontrollen. Dette gjelder for eksempel oversikt over ansvarsforhold og rutiner for ivaretagelse av de registrertes rettigheter (informasjon, sletting, etc.)

Etter at Datatilsynet mottok første brev fra PepCall AS med svar på de spørsmål som Datatilsynet hadde bedt om redegjørelse for gjensto flere av spørsmålene ubesvart. Dette gjaldt for eksempel spørsmål knyttet til oversikt over personopplysninger som behandles, klassifisering av disse, fastlagt kriterier for akseptabel risiko og risikovurderinger.

I tilsvar til varsel om vedtak har vi fått tilsendt en oppdatert internkontroll og beskrivelse av enkelte rutiner som for eksempel sletting. Som vist ovenfor legger vi også til grunn at PepCall AS for fremtidige kunder vil oppfylle informasjonsplikten. Kunder som etablert kundeforhold før denne informasjonen ble tilgjengelig har imidlertid ikke fått sin rett til informasjon oppfylt, og følgelig ikke muligheten til å gjøre et aktivt valg på bakgrunn av informasjonen.

PepCall AS mener at den oversendte dokumentasjonene viser at det ikke er grunnlag for å opprettholde pålegg om stans i behandling av personopplysninger på bakgrunn av manglende internkontroll.

Vi ser at det er gjort forbedringer ved at PepCall AS blant annet har igangsatt oppdatering av internkontrollen, oppdatere rutiner, igangsette risikovurderinger, inngåelse av avtaler med databehandlere og kontroll med underleverandører. Som påpekt ovenfor mener vi imidlertid at eksisterende kunder ikke er gitt muligheten til å ta informert valg med hensyn til bruk av tjenesten på grunn av manglende eller mangelfull informasjon. Ingen av de som var kunder før denne saken kom opp har fått sine rettigheter etter personvernregelverket oppfylt.

Plikten til å ha internkontroll innebærer også en plikt til å ha kjennskap til gjeldende regler om behandling av personopplysninger. Underveis i denne kontrollen er det avdekket at PepCall som tilbyder av teletjenester skulle hatt konsesjon fra Datatilsynet for denne virksomheten. Dette er ikke noe vi konkret stilte spørsmål ved i vårt krav om redegjørelse, og følgelig heller ikke noe som omfattes av påleggene. Fravær av konsesjon er imidlertid relevant i vurderingen av om internkontrollplikten er ivaretatt. Etter vår vurdering er det en indikasjon på manglende oversikt over hvilke plikter som påhviler en virksomhet som behandler beskryttelseverdige personopplysninger i den grad som PepCall AS gjør.

Vi kan ikke se at den internkontrollen som er lagt frem gir uttrykk for den helhetlige og systematiske tankegangen som vi mener må være på plass for en virksomhet som behandler så beskyttelsesverdig informasjon som dere gjør. Som redegjort for ovenfor etterlyser vi en mer helhetlig tankegang knyttet til vurdering av risiko ved behandling av personopplysninger. Det samme gjelder ivaretagelse av kundenes rettigheter og organisering av sikkerhetsarbeidet. På samme måte som det ikke er tilstrekkelig at sikkerhetshull blir lukket etter hvert som de blir avdekket av andre, så er det ikke tilstrekkelig å lage rutiner etterhvert som det blir avdekket at de mangler.

Dokumentasjonen som er tilsendt mener vi er klare indikasjoner på at PepCall AS ikke har etablert eller holdt ved like slike systematiske tiltak som skal til for å oppfylle pliktene etter personopplysningsloven, og følgelig ikke ivaretar rettighetene til de som det behandles personopplysninger om.

Konklusjon
Fravær av planlagte og systematiske tiltak for å oppfylle sine plikter og de registrertes rettigheter etter personopplysingsloven er i strid med kravene i personopplysningsloven § 14 og personopplysningsforskriften § 3-1.

Samlet vurdering
På bakgrunn av den tid som er gått siden PepCall AS først ble kjent med sikkerhetshullene i produktene som tilbys, fristen gitt for å svare på spørsmål om grunnleggende internkontroll, de mangelfulle svar som er gitt så mener vi det er nødvendig å fatte vedtak om opphør av ulovlig behandling av personopplysninger, jf. personopplysningsloven § 46, jf. personopplysningloven §§ 13, 14 og 19.

Tvangsmulkt
Vi vil vurdere bruk av tvangsmulkt dersom påleggene ikke er gjennomført innen fristen (jf. personopplysningsloven § 47).

Klagemulighet
Dere kan klage på vedtaket. En eventuell klage må sendes til oss **innen tre uker** etter at dette brevet er mottatt (jf. forvaltningsloven §§ 28 og 29). Dersom vi opprettholder vårt vedtak vil vi sende saken videre til Personvernnemnda for klagebehandling.

Innsyn og offentlighet
Dere har rett til innsyn i sakens dokumenter (jf. forvaltningsloven § 18). Vi vil også informere dere om at alle dokumentene i utgangspunktet er offentlige (jf. offentlighetsloven § 3), men understreker samtidig at sikkerhetsdokumentasjon som hovedregel er unntatt offentlighet (jf. offentlighetsloven § 13, jf. personopplysningsloven § 45).

Hvis dere har spørsmål, kan dere ta kontakt med Eirin Oda Lauvset på telefon 22 39 69 11.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Eirin Oda Lauvset
seniorrådgiver