Datatilsynet

GPS for barn - Smartprodukt AS
Gokstadveien 18

3216 SANDEFJORD

Deres referanse	Vår referanse	Dato
	17/01483-17/EOL	18.12.2017

Pålegg om stans av behandling av personopplysninger - Smartprodukt AS (GPS for barn)

Vi viser til vårt brev av 7. desember med varsel om pålegg, og deres svar mottatt 13. desember 2017.

Vi forstår deres svar dithen at dere ikke har merknader til det som er lagt til grunn som fakta, og viderefører dermed beskrivelsen av sakens bakgrunn fra varselet.

I deres tilbakemelding ber dere om veiledning med hensyn til hvordan dere skal oppfylle informasjonsplikten ovenfor deres kunder. Datatilsynet har gitt dere veiledning underveis i denne saken, men slik vi ser det er mye av grunnlaget for de vedtak vi har varslet nettopp manglende forståelse for hvilke forpliktelser deres virksomhet har etter personvernregelverket. Vi er av den oppfatning at vi har oppfylt vår veiledningsplikt, og vi fastholder dermed vårt varslede vedtak.

Vedtak om pålegg
Datatilsynet vedtar følgende pålegg:

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

2. Smartprodukt AS må stoppe all behandling av personopplysninger som er i strid med personopplysningsloven § 13. Smartprodukt AS har ikke sørget for tilfredsstillende informasjonssikkerhet med hensyn til vern av konfidensialitet og integritet for kunders personopplysninger lagret ved bruk av Viksfjord og andre klokker tilknyttet GPSFORALLE eller SeTracker.

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

3. Smartprodukt 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.

   Smartprodukt 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 pålegget er **8. januar 2018.** Innen denne fristen må dere sende oss en skriftlig bekreftelse på at pålegget er gjennomført.

Nærmere om sakens faktiske forhold
Smartprodukt AS er ansvarlig markedsfører av Viksfjord, og andre klokker, tilknyttet en app ved navn SeTracker 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 (sanntid og historikk).

Forbrukerrådet gjorde tidligere i høst en undersøkelse av sikkerheten i ulike typer GPS-klokker som er tilgjengelige på det norske markedet. En av klokkene som ble undersøkt var Viksfjord, som markedsføres av Smartprodukt AS. Det ble gjort funn som at det blant annet var mulig for uvedkommende å få ut informasjon fra klokken, det var mulig å avlytte klokken, samt se og endre lokasjon, og få tilgang til historiske lokasjonsdata. Det var også mulig å registrere klokken på en ny konto uten at den eksisterende eieren får noen indikasjon på at dette har skjedd.

På bakgrunn av Forbrukerrådets undersøkelser og funn rettet Datatilsynet en henvendelse til Smartprodukt 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, men en bredere kontroll av hvordan Smartprodukt AS ivaretar kundenes personvern og sørger for tilfredsstillende informasjonssikkerhet for alle tilsvarende produkter som virksomheten tilbyr på markedet.

I sitt tilsvar hevder Smartprodukt AS at sikkerhetshull er lukket og at det nye lagringsstedet for data fra smartklokkene ikke skal være mulig å kompromittere. Smartprodukt har også informert om at de nå har gått over til en ny app, GPSFORALLE.

Forbrukerrådet har fått gjennomført en ny undersøkelse av Viksfjord og den nye GPSFORALLE appen for å kontrollere påstandene om at krav til informasjonssikkerhet er ivaretatt. I en rapport mottatt 24. november 2017, fremgår det at deres undersøkelser viser at det fortsatt er sikkerhetshull i løsningen deres og at de i tillegg har funnet nye alvorlige sårbarheter.

Smartprodukt har ikke kommet med noen korrigeringer til den beskrivelsen av de faktiske forhold som fremgikk av varsel om vedtak. Vi legger derfor til grunn dette som faktum i saken.

Krav i regelverket og Datatilsynets vurdering
I det følgende vil vi gjennomgå de aktuelle reglene og gjøre rede for vår vurdering av om reglene er fulgt i denne konkrete saken.

Nærmere om personopplysningslovens krav til 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 bl.a. 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 Smartprodukt 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, avlytting, etc) og kontinuerlig lokasjon. Dette tilsier at informasjonssikkerheten skal være høyt prioritert og på et høyt nivå.

De sikkerhetshull som er avdekket av Forbrukerrådet i samarbeid med mnemonic er svært graverende. Det er blant annet avdekket at det er mulig for uautoriserte å bruke informasjonssystemet uten at det er mulig å oppdage. I følge personopplysningsforskriften § 2-14 har Smartprodukt AS en eksplisitt plikt til å iverksette tiltak for å oppdage slik bruk.

Personopplysningsforskriftens §§ 2-11 og 2-13 fastslår videre virksomhetens plikt til å sørge for henholdsvis opplysningenes konfidensialitet og integritet. Det at informasjonssystemet har vært mulig for uautoriserte å bruke uten at det er mulig å oppdage betyr at personopplysningene har vært tilgjengelige og mulig å endre/manipulere for uvedkommende. Svarene vi har mottatt fra Smartprodukt inneholder ingen dokumentasjon som viser at ledelsen i Smartprodukt har vurdert risiko eller tatt stilling til i hvilken grad restrisiko er akseptabel for sin virksomhet.

Smartprodukt har altså ikke gjort noen egen risikovurdering basert på egen interkontroll og oversikt over personopplysninger, verdivurdering og trusler. Smartprodukt hevder for eksempel at personopplysninger kun lagres innen EU (Tyskland), mens det utfra øvrige beskrivelser av tjenesten går frem at 3G Electronics i Kina hoster servere og utvikler applikasjonen, noe som vanligvis betyr at de også har tilgang til personopplysningene som behandles i appen. For behandling av personopplysninger i Kina skulle det vært informert spesifikt til kundene om dette, samt at det skulle vært inngått databehandleravtale og standardavtale for utlevering av personopplysninger ut av EU.

Smartprodukt har ikke sendt over noe informasjon som tyder på at de 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. Vi stiller oss spørrende til om de har kontroll med om det brukes for eksempel løsninger og APIer fra tredjeparter til bruk av kart, og hvilke personopplysninger som sendes over og hvor de lagres. I sitt svar fremgår det også relasjoner til virksomhetene Dealhonor technologies og Anquanshouhu technologies som ser ut til å befinne seg i henholdsvis Hong Kong og Kina uten at det er nærmere beskrevet hvordan disse relasjonene er formalisert. I «User guidelines» i appenes «Privacy policy» fremgår det videre at programvare er bundlet med klokke fra henholdsvis Dealhonor (GPSFORALLE) og Anquanshouhu (SeTracker), at den bruker innebygd Google Map og rapporterer lokasjon til Dealhonor eller Anquanshouhu uten at disse relasjonene er nærmere beskrevet eller formalisert. I siste rapport fra mnemonic går det dessuten frem at opplysninger sendes til asia.myaqsh.com i Singapore. Hva som er formålet med denne utvekslingen, hvem som har tilgang og hva de bruker opplysningene til her er heller ikke redegjort for.

Dette er informasjon som tyder på at personopplysninger utveksles i større grad enn det Smartprodukt AS har redegjort for.

Som behandlingsansvarlig skal Smartprodukt være i forkant og iverksette planlagte og systematiske tiltak for å ivareta informasjonssikkerheten. Det er ikke tilstrekkelig å inngå avtaler og lukke avvik etterhvert som mangler blir påvist av andre.

Som behandlingsansvarlig skulle Smartprodukt 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.

Etter Datatilsynets oppfatning har ikke Smartprodukt AS planlagte og systematiske tiltak som er egnet til å håndtere den sikkerhetsrisiko som produktene deres innebærer for behandling av personopplysninger. Dersom slike hadde vært på plass så ville Smartprodukt AS vært i stand til å oppdage den type graverende sikkerhetshull som mnemonic har påvist, og disse ville vært avdekket før informasjonssystemet ble tatt i bruk. Vi ser heller ingen indikasjoner på at Smartprodukt AS har oversikt over det totale økosystemet hvor personopplysningene som genereres av smartklokkene befinner seg.

Eksempler på manglende kontroll og forankring omtales også senere i brevet da dette er en grunnleggende feil som materialiserer seg på flere områder.

Vår vurdering er at Smartprodukt ikke har hatt tilstrekkelig eierskap til, eller kontroll med behandling av personopplysninger i sine produkter og informasjonssystem.

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.

Personopplysningsloven §§ 18 og 19 om plikt til å gi informasjon og Datatilsynets vurdering
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 Smartprodukt AS forelå det ingen informasjon tilgjengelig om hvordan Smartprodukt AS behandler personopplysninger ved kunders bruk av deres produkter. Etter vårt krav om redegjørelse er det laget en personvernerklæring, men informasjonen i denne tilfredsstiller ikke kravene i personopplysningsloven §§ 18 og 19. I denne saken er for eksempel ansvarsforhold og relasjoner mellom ulike virksomheter (behandlingsansvarlige, databehandlere, leverandører, teleoperatører, etc) vanskelig å få oversikt over. 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 får de ikke. Det fremgår 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 ekstrafunksjonalitet, om opplysninger deles med andre virksomheter, hvordan kundene kan utøve sine rettigheter (innsyn, trekke samtykke, slette data etc.).

Smartprodukt informerer om at personopplysninger kun sendes kryptert til servere i Tyskland. Som redegjort for over mener vi at dette ikke stemmer overens med andre opplysninger i saken, for eksempel at samarbeidspartnere i Kina, Hong Kong og Singapore kan ha tilgang til personopplysninger.

Dette betyr at kunder som har kjøpt klokker før november 2017 ikke har fått noen informasjon, mens kunder som har kjøpt klokker etter november 2017 har fått mangelfull og villedende informasjon, jf informasjonen over.

Ved nedlasting av appene SeTracker og GPSFORALLE finnes det «Privacy policy» som ser helt like ut, bortsett fra at SeTracker refererer til Aquanshouhu Technologies og GPSFORALLE refererer til Dealhonor Technologies. I et slikt dokument ville vi forventet 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 finner er 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.

For øvrig må vi bemerke at mesteparten av dokumentet handler om opphavsrettslige forhold, og ikke personvernrettslige forhold. Dette er noe underlig, og også misvisende all den tid lenken til dokumentet heter «personvernregler».

På bakgrunn av ovennevnte mener Datatilsynet at kunder som har kjøpt smartklokker fra Smartprodukt AS ikke har vært gjort i stand til å gjøre informerte valg.

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

Personopplysningsloven § 14 om plikt til å ha internkontroll og Datatilsynets vurdering
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.)

Datatilsynet har mottatt et tilsvar fra Smartprodukt AS med noen svar på de spørsmål som Datatilsynet har bedt om redegjørelse for. I lys av de funn som Forbrukerrådet har gjort i sin nye undersøkelse, gir ikke den mottatte redegjørelsen tilstrekkelige garantier for personvern og informasjonssikkerhet. Etter vår vurdering gjenstår dessuten flere av våre spørsmål ubesvart. Dette gjelder for eksempel spørsmål 1–3 om oversikt over personopplysninger som behandles, klassifisering av disse, fastlagt kriterier for akseptabel risiko og risikovurderinger. Vi registrerer at Smartprodukt har laget noe informasjon på sine nettsider om hvordan de behandler personopplysninger, men denne informasjonen tilfredsstiller som nevnt over ikke informasjonsplikten i personopplysningsloven §§ 18 og 19.

Når det gjelder sletterutiner sier Smartprodukt AS at de har automatisk sletting av data på serverne til 3G Electronics (posisjonering osv.) etter 365 dager. Denne sletterutinen er verken knyttet til konkrete opplysninger eller formål, og vitner om fravær av forståelse for hensynet bak disse pliktene. Uten konkrete rutiner/avtaler med de ulike delene av økosystemet hvor opplysningene befinner seg må denne påstanden om sletting uansett anses udokumentert.

Det Smartprodukt AS har redegjort for oppfyller ikke plikten til å sørge for sletterutiner for de enkelte kategorier av opplysninger relatert til de formål de er innhentet, jf. personopplysningsloven § 14, jf. personopplysningsforskriften § 3-1 tredje ledd bokstav c.

De mangelfulle svar som er gitt mener vi er klare indikasjoner på at Smartprodukt 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 Smartprodukt 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 og Forbrukerrådets nye rapport om vedvarende sikkerhetsbrister, så mener vi det er nødvendig å varsle 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

Kopi til: Forbrukerrådet, Postboks 463 Sentrum, 0105 OSLO