Datatilsynet

Gator AS
Håkon Magnussons gate 8
7041 TRONDHEIM

Deres referanse	Vår referanse	Dato
	17/01432-12/EOL	07.12.2017

Pålegg om stans av behandling av personopplysninger - Gator AS

Vi viser til vårt brev av 18. oktober 2017 med krav om redegjørelse, deres svar 10. november 2017, og vårt varsel om vedtak av 16. november 2017. Vi mottok deres merknader til varselet den 24. november 2017. Våre kommentarer til merknadene følger under.

Vedtak om pålegg
Datatilsynet vedtar følgende pålegg:

1. Gator AS må stoppe all behandling av personopplysninger om sine kunder fordi den er i strid med personopplysningsloven §§ 13-15. Gator AS har ikke sørget for tilfredsstillende informasjonssikkerhet med hensyn til vern av konfidensialitet og integritet for kunders personopplysninger lagret ved bruk av smartklokkene de leverer.

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

Vår hjemmel for å fatte pålegg er personopplysningsloven § 46.

Fristen for å gjennomføre pålegget er **29. desember 2017.** Innen denne fristen må dere sende oss en skriftlig bekreftelse på at pålegget er gjennomført.

Nærmere om sakens faktiske forhold
Gator AS er ansvarlig markedsfører av produktene Gator 2 og 3 på det norske markedet. Dette er smartklokker 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 Gator 2. 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 å se 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 Gator 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 Gator AS ivaretar kundenes personvern og sørger for tilfredsstillende informasjonssikkerhet for alle tilsvarende produkter som virksomheten tilbyr på markedet.

I sitt tilsvar hevder Gator AS at sikkerhetshull er lukket og at det nye lagringsstedet for data fra smartklokkene ikke skal være mulig å kompromittere. Forbrukerrådet har fått gjennomført en ny undersøkelse av Gator 3 for å kontrollere denne påstanden. I en rapport mottatt 16. november 2017, fremgår det at undersøkelser viser at det fortsatt er sikkerhetshull i løsningen deres og at det i tillegg er funnet nye alvorlige sårbarheter. På denne bakgrunn fattet Datatilsynet et varsel om vedtak om at all behandling av personopplysninger må stanses.

Gator AS har kommet med merknader til Datatilsynets varslede vedtak, og mener det ikke lengre er grunnlag for å fatte vedtak om stans i behandlingen av personopplysninger. I det følgende vil vi gjennomgå grunnlagene for vedtak, Gator AS sine merknader og våre konklusjoner.

Nærmere om personopplysningslovens krav til informasjonssikkerhet
Etter personopplysningsloven § 13 skal den behandlingsansvarlige gjennom planlagte og 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 Gator 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 Gator AS en eksplisitt plikt til å iverksette tiltak for å oppdage slik bruk. Forskriften §§ 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 Gator AS inneholder ingen dokumentasjon som viser at ledelsen i Gator AS har vurdert og tatt stilling til i hvilken grad restrisiko er akseptabel for sin virksomhet. Redegjørelsen viser derimot at konsulenter og samarbeidspartnere har gjort vurderinger og tatt beslutninger på vegne av Gator AS.

I sitt svarbrev informerer Gator AS om at det er foretatt risikovurderinger og inngått avtaler med samarbeidspartner Tech SixtyFour og konsulentselskapet Intruder Ltd. som skal sørge for at informasjonssikkerheten blir ivaretatt for klokkene med tilknyttet applikasjon. Det er avtalt månedlige sikkerhetsrevisjoner av Gator AS sine systemer, samt at det er inngått avtale med Evry for test av ny applikasjon.

Det er positivt at Gator AS har fått gjennomført risikovurderinger og at det er inngått avtaler med virksomheter med kompetanse på revisjon og sikkerhetstesting. Vi registrerer imidlertid at de to risikovurderingene vi har fått oversendt er av henholdsvis de sårbarhetene som mnemonic påviste og de gjenværende sårbarhetene som Intruder har påvist. Gator AS har altså ikke gjort noen egen risikovurdering basert på egen interkontroll og oversikt over personopplysninger, verdivurdering og trusler. Som behandlingsansvarlig skal Gator 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.

Som behandlingsansvarlig skulle Gator 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.

Etter Datatilsynets oppfatning har ikke Gator 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 Gator 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.

Et skjerpende element er at Gator AS fikk varsel fra en kunde om de samme sikkerhetshullene i august 2017, men valgte å ikke gjøre noe med dette.

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 Gator AS ikke har hatt tilstrekkelig eierskap til, eller kontroll med behandling av personopplysninger i sine produkter og informasjonssystem. Vi viser til redegjørelsen der det fremgår at det er henholdsvis Gator Group Co., Ltd, Tech Sixty Four Ltd og Intruder som har vært ansvarlige for sikkerhetsrevisjoner og risikovurderinger.

Gator AS har overlatt ansvaret for beslutninger som har betydning for kundenes personvern og informasjonssikkerheten knyttet til behandling av personopplysninger, til databehandler og konsulenter. Organiseringen av sikkerhetsarbeidet pulveriserer 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.

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.

På det tidspunktet Datatilsynet ba om redegjørelse fra Gator AS forelå det ingen informasjon tilgjengelig om hvordan Gator AS behandler personopplysninger ved kunders bruk av deres produkter.

Etter vårt varsel om vedtak har Gator AS utarbeidet en personvernerklæring som er vedlagt deres merknader. Informasjonen i personvernerklæringen 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, og hvilke kategorier av personopplysninger som overføres hvor. 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. Vi kan for øvrig ikke se at denne informasjonen er tilgjengelig.

Ved nedlasting av app i Appstore finnes det ingen informasjon om personvernregler. Ved nedlasting av app fra Google Play finnes det riktignok en lenke som heter «Personvernregler». I et slikt dokument ville vi imidlertid 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.

I tillegg til at personvernerklæringen er mangelfull og lite tilgjengelig så inneholder den informasjon om rettslige forhold som er direkte misvisende. I personvernerklæringen informeres det om at Gator AS bruker informasjon om kundene sine for å
- overvåke trender og bruk
- tilpasse markedsføring mot enkeltkunder
- bruke informasjon som de har samlet inn fra informasjonskapsler eller annen teknologi, til å forbedre tjenestene.

Vi legger til grunn at det rettslige grunnlaget for Gator AS sin behandling av personopplysninger om kunder er personopplysningsloven § 8 bokstav a, at behandlingen er nødvendig for å oppfylle en avtale med den registrerte. Behandlingene nevnt over er ikke nødvendige for å oppfylle avtalen, og de har følgelig ikke noe rettslig grunnlag med mindre Gator AS har innhentet spesifikt samtykke fra sine kunder om slik behandling. Det er ikke noe i dokumentasjonen som tilsier at Gator AS har innhentet samtykke for behandling av personopplysninger for nevnte formål. Dette betyr at Gator AS behandler personopplysninger om sine kunder uten rettslig grunnlag.

Behandling av personopplysninger for formål utover det som er nødvendig for avtalen er i tillegg også nevnt i standardavtalen for overføring av personopplysninger til tredjeland som er inngått mellom Gator AS og Gator Group Co., Ltd. Vi gjør oppmerksom på at standardavtalen kun er hjemmel for overføringen av opplysninger, og gir ikke hjemmel til behandlingen i seg selv. Uten rettslig grunnlag for behandling av personopplysninger er behandlingen ulovlig. Vi legger til grunn at denne avtalen innebærer at de nevnte analysene blir gjennomført i Kina hos Gator Group Co., Ltd. Vi kan ikke se at Gator AS informerer sine kunder om at deres personopplysninger er tilgjengelig for samarbeidspartnere i Kina.

På bakgrunn av ovennevnte mener Datatilsynet at kunder som har kjøpt smartklokker fra Gator 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
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 18. 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 en påpeking av at flere av spørsmålene gjensto ubesvart mottok vi noen svar fra Gator AS i tilsvar til varslet vedtak. Standardavtalen som Gator AS har inngått med Gator Group Co., Ltd for overføring av personopplysninger til Kina reiser imidlertid flere spørsmål og synliggjør også motstrid i Gator AS påstander om etterlevelse av personvernregelverket.

Som nevnt over er det slik at standardavtalen kun er hjemmel for overføringen av opplysninger, og gir ikke hjemmel til behandlingen i seg selv. Uten rettslig grunnlag for behandling av personopplysninger er behandlingen ulovlig.

Vi kan heller ikke se at det er inngått databehandleravtale eller at tilgang til personopplysninger for de ansatte i den kinesiske virksomheten er regulert.

I standardavtalen er det nevnt at det kan brukes underleverandører, men siden vi ikke har sett noen databehandleravtale, stiller vi spørsmål til hva slags oversikt Gator AS har over «økosystemet» til utvikling og drift av klokker, apper og servere. 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 sendes over og lagres hvor. I den siste rapporten utført av mnemonic stod det dessuten at det så ut som en av serverne ble driftet i en Amazon AWS sky i USA. Dette reiser nye spørsmål om oversikt, kontroll og avtaleinngåelser.

Der er videre opplyst at den nye appen skal lagres hos Amazon innenfor EU, men det er ikke redegjort for ansvar og sikkerhet med hensyn til utvikling og vedlikehold av appen, og drift av servere.

I lys av de funn som Forbrukerrådet har gjort i sine undersøkelser og de motstridende opplysningene som er kommet frem i saken har vi ikke tillit til Gator AS sine forsikringer om tilstrekkelige garantier for personvern og informasjonssikkerhet. De mangelfulle svar som er gitt og Forbrukerrådets nye rapport om vedvarende sikkerhetsbrister mener vi er klare indikasjoner på at Gator 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 Gator 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 15.

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