Datatilsynet

Gator AS
Håkon Magnussons gate 8
7041 TRONDHEIM

Deres referanse	Vår referanse	Dato
	17/01432-22/EOL	10.01.2018

Frafall av pålegg om stans i behandling av personopplysninger og pålegg knyttet til videre oppfølging

Vi viser til vårt pålegg om stans av behandling av personopplysninger i brev av 7. desember 2017 med frist satt for gjennomføring til 8. januar 2018, deres tilbakemeldinger til pålegget av 21. desember 2017 samt etterfølgende e-postkorrespondanse med diverse avklaringer.

I deres tilbakemelding på vårt pålegg og medfølgende vedlegg gjøres det rede for det som er gjort for å få på plass rutiner for etterlevelse av personopplysningsloven med forskrift. Etter gjennomgang av denne dokumentasjonen og etterfølgende avklaringer ser vi at det fortsatt er gjenstående arbeid for å kunne si at virksomheten har etablert og implementert en fullverdig internkontroll. Vi er imidlertid kommet til at de gjenstående punktene ikke er alvorlige nok til å danne grunnlag for pålegg om stans av behandling av personopplysninger.

Vedtak om pålegg
Datatilsynet vedtar følgende pålegg:

1. Gator AS må etablere et klart skille mellom hvilken behandling av personopplysninger som er nødvendig for å gjennomføre avtalen med de registrerte og hvilken behandling av personopplysninger som må baseres på samtykke, jf. personopplysningsloven § 11, jf. § 8.

2. Gator AS må i sin informasjon til kunder gi klart uttrykk for skillet mellom hvilken behandling av personopplysninger som er nødvendig for å gjennomføre avtalen med de registrerte og hvilken behandling av personopplysninger som må baseres på samtykke, jf. personopplysningsloven § 18 første ledd bokstav c.

3. Gator AS må innhente samtykke fra sine kunder for å behandle personopplysninger for formål som går utover det som er nødvendig for å gjennomføre avtalen, jf. person personopplysningsloven § 11, jf. §8.

4. Gator AS må inngå databehandleravtale med leverandør av support/kontaktskjema (Zendesk), jf. personopplysningsloven § 15. Avtalen må være mer spesifikk på når utlevering av personopplysninger fra databehandler til tredjepart kan skje. Avtalen må også inneholde opplysninger om hvor data lagres, hvem får tilgang, hvilke underleverandører Zendesk bruker, hvor disse underleverandørene lagrer data etc.
5. Gator AS må informere sine kunder om at utviklere i Israel (United Perfectum) og leverandør av support/kontaktskjema i USA (Zendesk) har tilgang til personopplysninger, jf. personopplysningsloven § 19 første ledd bokstav c.
6. Gator AS må innen fristen forelegge status på fremdriftsplan i vedlegg 11 i svarbrevet fra Gator AS sendt 21. desember 2017.

Vår hjemmel for å fatte pålegg er personopplysningsloven § 46.

Fristen for å gjennomføre påleggene er satt i tråd med virksomhetens egen fremdriftsplan til **3. april 2018**. Innen denne fristen må dere sende oss en skriftlig bekreftelse på at påleggene er gjennomført.

Rettslig grunnlag for behandling av personopplysninger
Vi legger til grunn at det primære 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.

Behandling av personopplysninger for formål utover det som er nødvendig for gjennomføring av avtalen må baseres på andre rettslige grunnlag. Samtykke er et aktuelt rettslig grunnlag for behandling av personopplysninger som kan oppfylle vilkårene for gyldig samtykke.

I personvernerklæringen informeres det under punkt B om at enkelte opplysninger er det frivillig for kunden å oppgi (profilbilde, identifiserende opplysninger om bruker, kobling mot Facebook, kobling mot kontaktliste). Vi legger til grunn at Gator AS her mener at samtykke er rettslig grunnlag for behandling av disse opplysningene.

Under punkt C i personvernerklæringen går det frem at Gator AS også behandler detaljert informasjon om brukernes aktivitet på tjenesten, informasjon om enhetene som er i bruk, lokaliseringsinformasjon (inklusiv historikk) og logginformasjon uten at det er klargjort hva som er det rettslige grunnlaget for behandlingen.

Gator AS må gjøre det klart for sine kunder hvilken behandling av personopplysninger som er nødvendig for å oppfylle avtalen med kunden, og hvilken behandling av personopplysninger som eventuelt kan baseres på samtykke.

Behandling av personopplysninger med formålene overvåking av trender og bruk, tilpasset markedsføring mot enkeltkunder, bruke informasjon som er samlet inn fra informasjonskapsler eller annen teknologi, til å forbedre tjenestene 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 må innhente samtykke fra sine kunder til denne behandlingen.

Databehandlere, avtaler og informasjon
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.

I siste oversendelse fikk vi en avtale som gjelder leverandør av support/kontaktskjema, Zendesk. Vi har moen merknader til denne avtalen.

For det første er avtalen ikke signert av noen av partene. For det andre er det uklart hva avtalen tillater av bruk av personopplysninger. På side 1 står det at *«Zendesk only discloses Service Data to third parties where disclosure is necessary to provide the services or as required to respond to lawful requests from public authorities.»*. Avtalen må være mer presis enn dette på hva som legitimerer en utlevering av personopplysninger fra databehandler til tredjepart. Hvilke scenarier er det som kan nødvendiggjøre utlevering til tredjepart som en del av leveransen av tjenesten?

I personvernerklæringen er det kun Amazon og Svea Finans som er nevnt som databehandlere, mens vår e-post korrespondanse har avdekket at det i realiteten er langt flere databehandlere. Listen over databehandlere må altså suppleres.

I personvernerklæringen står det spesifikt at personopplysninger ikke vil bli overført ut av EU/EØS. Oversendt dokumentasjon viser imidlertid at databehandlerne Zendesk og United Perfectum lagrer data i henholdsvis USA og Israel. Informasjon til kundene, inkludert personvernerklæringen, må korrigeres på dette punktet. Informasjonen må være forståelig for at kundene skal forstå f.eks. hvilke type opplysninger som blir behandlet der og hva det innebærer.

Revisjon og jevnlige sikkerhetstester
Datatilsynet legger til grunn at Gator AS følger opp med revisjoner og sikkerhetstester slik det er beskrevet i fremdriftsplanen som er sendt oss (vedlegg 11). Som et generelt punkt minner vi om viktigheten av at Gator AS ved gjennomføring av revisjon av databehandlere, som Amazon, United Perfectum og Zendesk, forsikrer seg om at ikke personopplysninger blir overført fra den regionen dere har valgt. Dere må også kontrollere at databehandleravtalene dere har inngått går foran eventuelle privacy policies eller andre lignende avtaler. En viktig del av revisjonen er også å kontrollere om det brukes underleverandører, hvilke disse er, hvor de lagrer data, hva de har tilgang til, etc.

Når det gjelder sikkerhetstester ønsker vi innen samme frist en status på gjennomføring av slike og resultatet. Dersom det blir avdekket avvik som har medført uautorisert utlevering av

konfidensielle personopplysninger forutsetter vi at dette meddeles Datatilsynet i medhold av personopplysningsloven § 13, jf. personopplysningsforskriften § 2-6. Personopplysningene som behandles i deres produkt vil som utgangspunkt være å anse som konfidensielle, og en plikt til å melde avvik vil dermed for eksempel gjelde hvis en kunde har fått tilgang til en annen kundes personopplysninger gjennom bruk av smartklokke med tilhørende applikasjon.

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

Martha Eike
senioringeniør

Eirin Oda Lauvset
seniorrådgiver

Kopi til: Forbrukerrådet, Postboks 463 Sentrum, 0105 OSLO