

ORDR AS
Calmeyers gate 5

0183 OSLO

Deres referanse

Vår referanse
20/04292-1

Dato
18.11.2020

Krav om redegjørelse - betalingsformidling og smittesporing i serveringsbransjen - Ordr AS

Datatilsynets oppgave er å føre kontroll etter personopplysningsregelverket slik at enkeltpersoner ikke blir krenket gjennom bruk av opplysninger som kan knyttes til dem.

1. Sakens bakgrunn

Vi har registrert at Ordr AS («Ordr») leverer en salgs- og markedsføringsplattform som blant annet legger til rette for kontaktløs bestillingsformidling og betaling i serveringsbransjen.¹ Tjenesten har blitt særlig aktuell på grunn av den pågående koronapandemien ettersom serveringsstedene tar i bruk nye løsninger for kontaktløs bestilling og betaling for å minimere nærkontakt.

Tjenesten fungerer slik at brukerne skanner en QR-kode med telefonen sin. Deretter blir de videresendt til nettsiden app.ordr.no, en nettside med meny og bestillingssystem tilknyttet serveringsstedet man befinner seg på. Bestillinger kan også gjøres via nettsiden ordr.no. Betaling foretas med bankkort eller Vipps. Her kan man også registrere kontaktinformasjon for smittesporing.

Av nettsidene ordr.no framgår det at dere er tilknyttet serveringssteder over hele landet, og dere omtaler dere som «Norges raskest voksende plattform for mobil bestilling og betaling». Dere oppgir at dere er tilknyttet 400 brukersteder. I artikkelen i Finansavisen fra september kommer det også fram at dere hatt en vekst i transaksjonsvolum på 40.000 prosent i juli og august. Dere skriver også på nettsiden at dere tilbyr rapportering og avansert innsikt gjennom data i sanntid.

Vi har funnet lite konkret informasjon om hvilke personopplysninger Ordr behandler. På <https://ordr.no/cookies> har vi funnet informasjon om hvordan dere bruker informasjonskapsler til analyse og annonsering. Når det gjelder smittesporingen ser vi av

¹ Finansavisen 6. september 2020: <https://finansavisen.no/lordag/gruenderintervjuet/2020/09/05/7562848/edwin-fjeldtvedt-har-truffet-blink-med-ordr.no>.

<https://web.ordr.no/smittesporing> at dere samler inn informasjon om navn, telefonnummer, e-postadresse (kun Vipps), bord-/sete-/romnummer dersom det er oppgitt, kjøpstidspunkt og navnet på stedet kunden besøkte.

Det fremkommer ikke klart fra informasjonen på nettsidene om Ordr er behandlingsansvarlig for noen av disse personopplysningene eller om dere opptrer som databehandler for serveringsstedene.

På denne bakgrunn finner Datatilsynet det hensiktsmessig å se nærmere på Ordr sin behandling av personopplysninger, herunder rollefordeling mellom databehandler og behandlingsansvarlig, dataflyt og etablerte styringssystemer.

2. Rettslig bakgrunn

Behandlingsansvarlig og databehandler

En behandlingsansvarlig bestemmer alene, eller sammen med andre, formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. personvernforordningens artikkel 4 nr. 7. En databehandler handler på vegne av, og etter instruks fra, en behandlingsansvarlig, jf. personvernforordningens artikkel 4 nr. 8.

Dersom to eller flere behandlingsansvarlige i fellesskap fastsetter formålene med og midlene for behandlingen, er de felles behandlingsansvarlige, jf. personvernforordningens artikkel 26.

Skillet mellom behandlingsansvarlig og databehandler beror på hvordan virksomheten behandler personopplysningene.

Den behandlingsansvarlige har det primære ansvaret for å etterleve kravene i forordningen, og er overordnet ansvarlig for å overholde personvernprinsippene og regelverket. Dette fremkommer av ansvarlighetsprinsippet i forordningens artikkel 5. Den behandlingsansvarlige må derfor sørge for å etablere alle nødvendige organisatoriske og tekniske tiltak for å sikre at regelverket etterleveres til enhver tid, jf. artikkel 24. Den behandlingsansvarlige må kunne vise at den opptrer i samsvar med reglene, jf. artikkel 5 nr. 2.

Forholdet mellom en behandlingsansvarlig virksomhet og databehandleren skal være regulert i en databehandleravtale. Avtalen skal sikre at personopplysningene blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysninger. Kravene til en databehandleravtale følger av artikkel 28 i personvernforordningen.

Prinsipper for behandlingen av personopplysninger

Personvernforordningen oppstiller noen grunnleggende prinsipper, som alle som behandler personopplysninger må opptre i samsvar med.

Prinsippet om åpenhet i personvernforordningen artikkel 5 nr. 1 bokstav a innebærer at behandlingen av personopplysninger skal være oversiktlig og forutsigbar overfor den

registrerte. Den det behandles personopplysninger om skal være informert om at det behandles personopplysninger og hvordan disse behandles.

Artikkel 13 fastsetter hvilken informasjon som skal gis ved innsamling av personopplysninger fra de registrerte. Artikkel 14 fastsetter hvilken informasjon som skal gis til de registrerte dersom opplysningene ikke er samlet inn fra dem.

Informasjonen skal gis på en kortfattet, åpen, forståelig og lett tilgjengelig måte, og på et klart og enkelt språk, jf. artikkel 12.

Personopplysninger skal kun behandles for spesifikke, uttrykkelige, angitte og legitime formål, jf. artikkel 5 nr. 1 bokstav b. Ethvert formål med behandling av personopplysninger skal identifiseres og beskrives presist. Videre skal ikke personopplysningene viderebehandles på en måte som anses uforenelig med formålene personopplysningene ble samlet inn for.

Virksomheter plikter å begrense mengden innsamlede personopplysninger til det som er nødvendig, adekvat og relevant for å realisere formålet med behandlingen, jf. artikkel 5 nr. 1 bokstav c. Dersom identitetsopplysninger eller personopplysninger ikke er nødvendige for å oppnå formålet, følger det av dataminimeringsprinsippet at slike opplysninger ikke skal behandles.

Det følger av personvernforordningen artikkel 5 nr. 1 bokstav e at det er forbudt å behandle personopplysninger lenger enn det som er nødvendig for å oppnå det fastsatte formålet. Personopplysninger som ikke lenger er nødvendige for formålet skal slettes eller anonymiseres.

Behandlingsgrunnlag

Personvernforordningen artikkel 6 nr. 1 krever at all behandling av personopplysninger har et lovlig behandlingsgrunnlag. Mulige behandlingsgrunnlag fremkommer av bokstav a til f i samme bestemmelse. Virksomheten må ha identifisert det rettslige grunnlaget for behandlingen på forhånd.

3. Vi ber om svar på følgende:

1. Hvilke personopplysninger behandler dere og for hvilke formål behandles de? Skill mellom smittesporing, betalingsformidling og eventuelle andre behandlinger.
2. Hva er behandlingsgrunnlagene for de ulike personopplysningene dere behandler, jf. artikkel 6 nr. 1?
3. For hvilke behandlinger anser dere at dere er behandlingsansvarlig, og for hvilke behandlinger er dere databehandler?
4. Vi ber om at dere sender over eksempel på en databehandleravtale dere har med et serveringssted. Hvis dere anser at dere har felles behandlingsansvar med serveringsstedene ber vi om at dere sender oss vurderingen av dette og ansvarsfordelingen dere imellom.
5. Vi ber om at dere redegjør kort for styringssystemet dere har implementert for å sikre at dere etterlever forpliktelsene deres etter personvernforordningen, jf. artikkel 24.

6. Vi ber om at dere sender oss behandlingsprotokollen, jf. artikkel 30, og at dere illustrerer dataflyten i løsningen, for eksempel i form av UML-diagrammer.
7. Vi ber om at dere sender over personvernerklæringen for plattformen, jf. artikkel 13.

Videre fremdrift

Dere må svare på spørsmålene våre og sende den etterspurte dokumentasjonen innen **10. desember 2020**.

Vern mot selvinkriminering

I tråd med forvaltningsloven § 48 gjør vi dere oppmerksom på at dere kan ha rett til ikke å svare på spørsmål eller utlevere dokumenter når svaret eller utleveringen vil kunne utsette dere for overtredelsesgebyr.

Hjemmelsgrunnlag

Etter personvernforordningen artikkel 58 nr. 1 og personopplysningsloven § 20, tredje ledd bokstav b har vi myndighet til å kreve de opplysningene som trengs for at vi skal kunne gjennomføre oppgavene våre.

Klageadgang

Dere kan klage på pålegget om å gi oss informasjon. En eventuell klage må sendes til oss innen tre dager etter at dette brevet er mottatt (jf. forvaltningsloven § 14). Dersom vi opprettholder vårt vedtak vil vi sende saken videre til Personvernemnda for klagebehandling.

Offentlighet, innsyn og taushetsplikt

Vi vil informere dere om at alle dokumentene i utgangspunktet er offentlige (jf. offentlighetsloven § 3). Dersom dere mener det er grunnlag for å unnta hele eller deler av dokumentet fra offentlig innsyn, ber vi dere om å begrunne dette.

Mer informasjon om personvern, internkontroll og informasjonssikkerhet kan dere finne på våre nettsider, www.datatilsynet.no.

Hvis dere har spørsmål, kan dere ta kontakt med Berit Bye Rinnan på telefon 22 39 69 58.

Med vennlig hilsen

Ylva Marrable
seksjonssjef

Berit Bye Rinnan
juridisk rådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer