Datatilsynet

Styreleder på vegne av styret,
FERDE AS
Postboks 2623 Møhlenpris
5836 BERGEN

Deres referanse	Vår referanse	Dato
	20/01727-3	27.09.2021

Vedtak om overtredelsesgebyr - Ferde AS

Datatilsynet viser til vårt varsel om vedtak om overtredelsesgebyr av 4. mai 2021 og merknadene deres til dette varselet av 20. mai 2021.

Basert på tilgjengelig informasjon har vi valgt å fokusere på spørsmål knyttet til eksistensen av databehandleravtale, risikovurdering samt overføringsgrunnlag for overføring av personopplysninger til tredjeland. Datatilsynet har ikke vurdert andre forhold knyttet til Ferde sin behandling av personopplysninger.

1. Vedtak om overtredelsesgebyr

Datatilsynet vedtar følgende:

> *I medhold av personvernforordningen artikkel 58 nr. 2 bokstav i, jf. personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 83, ilegges Ferde AS et overtredelsesgebyr på 5 000 000 NOK – fem millioner norske kroner – til statskassen, for overtredelse av kravene til databehandleravtale, risikovurdering og overføringsgrunnlag ved behandling av personopplysninger, jf. personvernforordningen artikkel 28 nr. 3, artikkel 32 nr. 2, jf. artikkel 5 nr. 1 bokstav f og artikkel 5 nr. 2, og artikkel 44 i en periode mellom ca. 12 – 25 måneder.*

2. Beskrivelse av sakens faktiske forhold

Gjennom NRK har Datatilsynet blitt kjent med at Ferde AS («Ferde») overfører opplysninger knyttet til passering i bomringer til en databehandler i Kina.[1] På denne bakgrunn initierte Datatilsynet en tilsynssak av eget initiativ.

[1] NRK.no: «Bomselskapet betalte 1,4 millioner kroner til den ansattes firma: Så tok kona over», 25. oktober 2019. https://nrk.no/norge/bomselskapet-betalte-1_4-millioner-kroner-til-den-ansattes-firma_-sa-tok-kona-over-1.14754802, sist åpnet 06. april 2021.
NRK.no: «Slike bilder sender bomselskap til Kina: Nå går Datatilsynet inn i saken», 28. oktober 2019. https://nrk.no/norge/slike-bilder-sender-bomselskap-til-kina_-na-gar-datatilsynet-inn-i-saken-1.14754918, sist åpnet 06. april 2021.

Basert på tilgjengelig informasjon har vi valgt å fokusere på spørsmål knyttet til eksistensen av databehandleravtale, risikovurdering samt overføringsgrunnlag for overføring av personopplysninger til tredjeland. Datatilsynet har ikke vurdert andre forhold knyttet til Ferde sin behandling av personopplysninger.

Den 29. oktober 2019 sendte vi et krav om redegjørelse der vi ba om informasjon om hvilke opplysninger som blir overført, hvilke garantier databehandleren har oppstilt for at personvernreglene følges samt hvilket overføringsgrunnlag Ferde har for å sende personopplysninger ut av EØS.[2] Vi ba også om å få se databehandleravtalen mellom Ferde og databehandleren i Kina samt dokumentasjon knyttet til overføringsgrunnlaget.

Beskrivelsen av sakens faktiske forhold bygger på Ferdes svar på krav om redegjørelse datert 6. november 2019 med vedlegg,[3] informasjon gjennom oppgitte NRK-artikler,[4] samt Kluges rapport «Vurdering av forhold i Ferde AS» av 4. desember 2019. Kluges rapport bygger på dokumentasjon som er fremlagt av Ferde, samt informasjon som har kommet frem gjennom intervjuer med ansatte i Ferde.

2.1. Om Ferde og deres virksomhet

Ferde er et regionalt bompengeselskap med mandat til å blant annet drive inn bompenger i sitt regionsområde. Selskapet ble stiftet med virkning fra 1. januar 2018 og overtok den manuelle billedbehandlingstjenesten i september 2017.[5]

Som ledd i sitt arbeid har Ferde ansvar for å registrere passeringer i bomstasjoner. Når brikken i biler som passerer Ferde sine bomstasjoner ikke blir korrekt registret eller bilen ikke har brikke, blir det tatt bilde av registreringsnummeret på bilen.

NRK.no: "Rapport etter NRK-avsløringer konkluderer: Flere regelbrudd i bomselskapet Ferde", 04. desember 2019. https://www.nrk.no/norge/rapport-etter-nrk-avsloringer-konkluderer_-flere-regelbrudd-i-bomselskapet-ferde-1.14807779, sist åpnet 06. april 2021.

[2] EØS består av EU-landene, Norge, Island og Liechtenstein.

[3] Vedleggene bestod av følgende dokumenter:

- Databehandleravtale mellom Ferde AS og Unitel Bratseth Services, ikke datert
- Driftsavtalen
- EUs standardkontraktsbestemmelser, inngått mellom Ferde AS (dataeksportøren) og Unitel Bratseth Services (dataimportøren), ikke datert, men inngått etter personverndirektivet (direktiv 05/46/EF).
- Konkurransegrunnlaget
- Mal for egenerklæring og taushetsplikt
- Mal for avvikshåndtering
- Mal for tilbudsbrev
- Risikovurdering, ikke datert
- Sladdet tilbudsbrev, datert 22.04.2019
- Sladdet tjenestekontrakt med vedlegg, datert 22.05.2019, inkludert:
    - Databehandleravtale
    - 10 bilag med underdokumenter

[4] Se fotnote 1.

[5] Av Kluges rapport (s. 10) opplyses det at etter en rekke sammenslåinger av ulike bompengeselskap ble aksjene i BT Signaal AS ble kjøpt med virkning fra 29. september 2017, og selskapet Ferde AS stiftet med virkning fra 1. januar 2018.

Disse bildene blir så sendt til automatisk optisk tegngjenkjenning for å digitalt lese nummerskiltet. I de tilfeller der bildekvaliteten ikke er tilstrekkelig god til at automatisk tolkning kan gjennomføres, blir bildet overført til manuell behandling. Ferde har kontrakt med Unitel Bratseth Services (heretter «UBS») om manuell bildebehandling (mer informasjon om dette under punkt 2.2.).

For den manuelle behandlingen benyttes IKT-løsningen levert at Q-Free, hvor løsningen driftes fra Norge, og alle data er lagret i Norge. Tilgangen til opplysninger i Q-Free avhenger av om man har rollen som såkalt «operatør» eller «supervisor».

Av bilag 1 til tjenestekontrakten med UBS (s. 1) fremgår det at Ferde, med utgangspunkt i historiske data, estimerte følgende årlige behov for manuell databehandling:

- Ca. 10 000 000 bilder til normalbehandling
- Ca. 2 500 000 bilder til oppfølgingsbehandling

2.2. Om personopplysninger, behandlingsansvarlig, databehandler og databehandleravtale

Ferde legger til grunn at bilskilt er en personopplysning. Bildene som behandles viser nedre del av bil, inkludert nummerskilt. Øvrige deler av bilen er sladdet, slik at fører ikke identifiseres. Utover dette ligger det informasjon om passeringstidspunkt, samt en numerisk kode for hvilken stasjon som er passert. Utover disse opplysningene som ligger i selve bildet, har ikke operatørene tilgang til andre opplysninger i løsningen.

På spørsmål om hvilke databehandlere Ferde bruker til å «punche» inn bilskilt manuelt, opplyser Ferde at de har en avtale med UBS om manuell bildebehandling. Dato for inngåelsen av databehandleravtalen er ikke oppgitt. Ferde oversendte databehandleravtalen inngått med UBS til Datatilsynet, men denne er ikke datert.

Av Kluges rapport (s. 21-22) fremgår følgende:

> *«Vi konstaterer at det er inngått en databehandleravtale (...) mellom Ferde og UBS. Dokumentene er ikke datert, men er opplyst å være inngått i forbindelse med oppstart av gjeldende avtale om MIR [Manuell billedbehandling] i 2019. Det foreligger også en tidligere versjon av en databehandleravtale mellom partene, som er opplyst signert i september 2018.»*

Kluge konkluderer (s. 8) med at det forelå manglende databehandleravtale i perioden fra Ferdes overtakelse av den manuelle billedbehandlingstjenesten i september 2017 frem til den først kom på plass i september 2018.

2.3. Personopplysningssikkerhet og risikovurdering

Hva gjelder garantier som Ferdes databehandlere har oppstilt i tråd med personvernforordningen artikkel 28 nr. 1, opplyser Ferde at UBS innga tilstrekkelige garantier etter bestemmelsen, gjennom tilbudet som ble levert under en offentlig anbudskonkurranse. Ferde har lagt disse garantiene til grunn i deres risikovurdering. Ferde har ovenfor Datatilsynet ikke opplyst nærmere om disse vurderingene, men viste til anbudsdokumentene, tilbud, kontrakt og risikovurdering.

I «sladdet tilbudsbrev» datert 22. april 2019 oppgir USB blant annet at:

> *«Selskapet har også høyt fokus på GDPR og alle ansatte får en innføring i hva dette vil si for hver enkelt og hvordan hver enkelt skal opptre for å ivareta sensitive data på en sikker og god måte. Bildebehandlerne har ikke fått kunnskap om hva metadataene i bildene betyr.*
>
> *Dette er gjort med vilje slik at ingen skal ha mulighet til kunne knytte en bompassering til en eksakt lokasjon. Alle ansatte må signere taushetserklæring før de kan starte i jobben.»*

Risikovurderingen som Ferde har inngitt til Datatilsynet er ikke datert.

I Kluge sin rapport (s. 21-22) er det oppgitt at:

> *«(…) det utarbeidet en relativt enkel og skjematisk risikovurdering fra Ferde knyttet til MIR i Kina. Ferde har i denne vurderingen konkludert med at det foreligger lav risiko for personvernkonsekvenser ved MIR i Kina. Risikovurderingen er ikke datert, men er opplyst å være utarbeidet omkring medio oktober 2019. (…) Det er ikke fremlagt dokumentasjon på, eller gitt informasjon om, at det tidligere har vært (…) foretatt risikovurderinger knyttet til MIR ved foregående avtaler med UBS/Bratseth E-commerce.»*

Kluge konkluderer (s. 8) med at det forelå manglende skriftlig risikovurdering i perioden fra Ferdes overtakelse av den manuelle billedbehandlingstjenesten i september 2017 frem til den først kom på plass i oktober 2019.

2.4. Overføring av personopplysninger utenfor EU/EØS

Ferde opplyser Datatilsynet at deres tjenesteleverandør av manuell billedbehandling, UBS, har ansatte i Kina som har tilgang til bildene og informasjonen knyttet til disse via web og via Ferde sine systemer. Ferde legger derfor til grunn at dette utgjør en overføring til tredjeland utenfor EØS.

Ferde angir at de benytter overføringsgrunnlaget i personvernforordningen artikkel 46 nr. 2 og at de, sammen med UBS, har signert EUs standardpersonvernbestemmelser. I oversendelsen til Datatilsynet vedla Ferde avtalen, men denne er ikke datert.
I Kluge sin rapport (s. 21-22) er det oppgitt at:

> *«Vi konstaterer at det er inngått en (…) standardavtale fra EU-kommisjonen mellom Ferde og UBS. Dokumentene er ikke datert, men er opplyst å være inngått i forbindelse med oppstart av gjeldende avtale om MIR i 2019. (…) Det er ikke fremlagt dokumentasjon på, eller gitt informasjon om, at det tidligere har vært signert standardavtale fra EU-kommisjonen».*

Kluge konkluderer (s. 8) med at det forelå manglende standardavtale fra EU-kommisjonen om utlevering til tredjeland i perioden fra Ferdes overtakelse av den manuelle billedbehandlingstjenesten i september 2017 frem til den først kom på plass våren 2019.

3. Rekkevidden av undersøkelsene og vurderingene

Som påpekt ovenfor har Datatilsynet opprettet tilsynssak av eget initiativ. I våre undersøkelser har vi fokusert på spørsmål knyttet til eksistensen av databehandleravtale, risikovurdering samt overføringsgrunnlag ved overføring av personopplysninger til tredjeland.

Vi har videre avgrenset våre undersøkelser av de faktiske forhold slik de var i tidsrommet september 2017 og frem til oktober 2019. Datatilsynet har med andre ord ikke sett på hvordan forholdene har vært etter oktober 2019. Datatilsynet har ikke vurdert andre forhold knyttet til Ferde sin behandling av personopplysninger, herunder innholdet i avtalene som er inngått, innholdet i risikovurderingen og kriteriene som følger av EU-domstolens dom i Schrems II-saken.[6]

4. Rettslig grunnlag

4.1. Om lovvalg

Den nye personopplysningsloven, som inkorporerer EUs personvernforordning i norsk rett, trådte i kraft 20. juli 2018. Loven opphevet samtidig personopplysningsloven (2000) og reglene i personopplysningsforskriften (2000).

Denne saken gjelder forhold som oppsto i 2017, altså før ikrafttredelsen av personopplysningsloven (2018), men som har vedvart i tiden etterpå. Vi må derfor ta stilling til om saken skal vurderes etter personopplysningsloven (2018) eller personopplysningsloven (2000).

I personopplysningsloven (2018) § 33 første ledd finnes en særskilt overgangsregel om overtredelsesgebyr, som lyder:

> *«Reglene om behandling av personopplysninger som gjaldt på handlingstidspunktet, skal legges til grunn når det treffes vedtak om overtredelsesgebyr. Lovgivningen på tidspunktet for avgjørelsen skal likevel anvendes når dette fører til et gunstigere resultat for den ansvarlige».*

Spørsmålet om lovvalg må altså vurderes ut fra hva som regnes som handlingstidspunktet.

De aktuelle manglende oppstod før ikrafttredelsen av nytt regelverk den 20. juli 2018, men vedvarte frem til oktober 2019. Handlingstidspunktet i denne saken har altså vedvart over tid og i tiden etter at personopplysningsloven (2018) trådte i kraft. Det følger da av personopplysningsloven (2018) § 33 at saken skal vurderes etter denne loven.

Vi viser også til forarbeidene til personopplysningsloven (2018), Prop. 56 LS (2017-2018) side 196, hvor departementet blant annet uttaler følgende om spørsmålet om lovvalg mellom personopplysningsloven (2000) og personopplysningsloven (2018):

[6] Sak C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems

«Utgangspunktet vil være at vedtak hos Datatilsynet og Personvernnemnda vil måtte fattes på grunnlag av de til enhver tid gjeldende materielle regler».

Det samme følger av Personvernnemndas praksis i saker som ble oversendt nemnda før ny lov trådte i kraft, men som ble behandlet etter ikrafttredelsen; se for eksempel PVN-2018-05 og PVN-2018-06.

På denne bakgrunn er det etter vår vurdering klart at saken må vurderes etter personopplysningsloven (2018) og personvernforordningen.

4.2. Om personopplysninger, behandlingsansvarlig, databehandler og databehandleravtale

Personopplysninger er alle opplysninger som kan knyttes til en enkeltperson, enten direkte eller indirekte. I de fleste tilfellene vil bilskilt være å regne for personopplysninger, siden bilen som hovedregel er knyttet til en navngitt eier og en begrenset krets av sjåfører. Bilens bevegelser vil for eksempel kunne avdekke eierens eller sjåførens aktiviteter og bevegelsesmønstre.

Den som bestemmer formålet med og midlene for behandling av personopplysningene, er såkalt behandlingsansvarlig. Den behandlingsansvarlige kan velge å sette ut behandling av personopplysninger til en såkalt databehandler.

Definisjonene av personopplysninger, behandlingsansvarlig og databehandler følger av personvernforordningen artikkel 4, jf. personopplysningsloven § 1.

Den behandlingsansvarlige har plikt til å kun bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen av personopplysninger oppfyller kravene i personvernforordningen. Det følger av personvernforordningen artikkel 28 nr. 1.

Videre skal det foreligge en databehandleravtale mellom den behandlingsansvarlige og eventuelle databehandlere. Dersom databehandleren benytter seg av underleverandører, skal en tilsvarende avtale foreligge mellom databehandleren og underleverandørene. Kravene til databehandleravtalens innhold, samt vilkårene for at en databehandler kan bruke underleverandører, fremgår av personvernforordningen artikkel 28.
Formålet med å ha på plass en databehandleravtale er å sikre at personopplysninger blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysninger. Databehandleravtaler skal dermed sørge for at både den behandlingsansvarlige og databehandleren forstår sine forpliktelser og sitt ansvar *før* behandlingen finner sted.

4.3. Risikovurdering

De grunnleggende prinsippene for behandling av personopplysninger fremgår av personvernforordningen artikkel 5. Vi viser særlig til artikkel 5 nr. 1 bokstav f, hvor det fremgår:

«1. Personopplysninger skal (...)

> *f) behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling (...), ved bruk av egnede tekniske eller organisatoriske tiltak («integritet og konfidensialitet»)».*

Det er behandlingsvarliges ansvar at prinsippene overholdes, og den behandlingsvarlige skal kunne påvise dette, jf. ansvarlighetsprinsippet i artikkel 5 nr. 2.

Både den behandlingsansvarlige og databehandlere har plikt til å påse at opplysningene behandles med tilstrekkelig informasjonssikkerhet, jf. personvernforordningen artikkel 32. Det følger videre av artikkel 32 nr. 2 at ved vurderingen av egnet sikkerhetsnivå skal tas «særlig hensyn til risikoene forbundet med behandlingen». Bestemmelsen oppstiller ingen form- eller innholdskrav til virksomhetens risikovurderinger. Det følger imidlertid av forordningen artikkel 5 nr. 2, jf. 5 nr. 1 bokstav f at den behandlingsansvarlige skal kunne påvise at opplysningen behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak. Det innebærer implisitt et krav om at risikovurderingene skal være dokumenterte og etterprøvbare, hvilket vil si at de må foreligge i skriftlig form og være datert.[7]

Arbeidet med informasjonssikkerhet må altså ta utgangspunkt i risikovurderinger av sannsynlighet for og konsekvenser av eventuelle avvik. Oppsummert skal en slik risikovurdering inneholde en vurdering av sannsynligheten for et sikkerhetsbrudd og hva slags konsekvenser det kan få.

Tidspunktet for når risikovurderingen skal være gjennomført på er ikke uttrykkelig regulert i artikkel 32. Plikten for behandlingsansvarlige til å gjennomføre en risikovurdering *før* personopplysninger behandles og *før* man tar i bruk et informasjonssystem kommer til imidlertid uttrykk i personvernforordningen artikkel 5 nr. 2, artikkel 24, artikkel 25 om innebygget personvern og artikkel 32 sett i sammenheng. For å reelt sett kunne håndtere sannsynlighet for og konsekvenser av eventuelle avvik og sikre god informasjonssikkerhet, må risikovurderingen være gjennomført før den faktiske behandlingen av personopplysninger skjer.

4.4. Overføring av personopplysninger utenfor EU/EØS

Det er i utgangspunktet ikke lov å sende personopplysninger ut av EU/EØS. Det finnes imidlertid unntak hvis det foreligger et eget grunnlag for overføringen i tråd med personvernforordningen kapittel 5. Ytterligere krav følger av den såkalte Schrems II-dommen.

Meningen med overføringsmekanismene er å pålegge dataimportøren en rekke plikter for å sikre at europeeres personopplysninger blir like godt beskyttet etter overførselen til tredjeland som de blir i EØS. Den som mottar opplysningene (dataimportøren) kan imidlertid være

[7] Skullerud, Åste Marie Bergseng mfl., *Personvernforordningen (GDPR) Kommentarutgave,* 1. utg., Universitetsforlaget, 2018, side 367.

underlagt lokale lover som er i strid med og går foran forpliktelsene etter overføringsgrunnlaget, eller det kan finnes andre omstendigheter som senker beskyttelsesnivået. Derfor må dataeksportøren i tillegg undersøke om beskyttelsesnivået som vil oppnås i praksis, faktisk er tilsvarende som i EØS.

Når det ikke foreligger en beslutning om tilstrekkelig beskyttelsesnivå, kan en overføring skje dersom den behandlingsansvarlig eller databehandler har gitt "nødvendige garantier", og under forutsetning av at den registrerte har håndhevbare rettigheter og effektive rettsmidler (jf. personvernforordningen art. 46 nr. 2.) Dette kan for eksempel sikres ved at den behandlingsansvarlige og databehandleren inngår en egen standardavtale som EU-kommisjonen har laget; EUs standardpersonvernbestemmelser.

Ved signering av EUs standardpersonvernbestemmelser forplikter dataimportøren seg til å behandle opplysningene i samsvar med de kravene som gjelder innenfor EU og EØS-området. Samtidig må dataeksportøren etablert i EU/EØS sjekke at personopplysningene som blir overført, faktisk får tilstrekkelig beskyttelsesnivå på lik linje som i EU/EØS før overføringen og at rettssystemet i mottakerlandet gjør det mulig å følge de standard personvernbestemmelsene i praksis.

Videre skal dataimportør opplyse eksportøren så fort som mulig om eventuelle hindringer for å oppfylle kravene. Et eksempel på en slik hindring er nasjonal lovgivning i tredjeland som kan gi offentlige myndigheter i tredjeland tilgang til personopplysninger utover det som anses nødvendig i et demokratisk samfunn (jf. fotnoten til artikkel 5 i de standard personvernbestemmelsene (2010/87/EU)). I så fall skal dataeksportøren ikke overføre personopplysningene i henhold til avtalen.

4.5. Særlig om ileggelse av overtredelsesgebyr

Av personvernforordningen artikkel 58 nr. 2 bokstav i) fremgår det at Datatilsynet kan ilegge overtredelsesgebyr etter reglene i personvernforordningen artikkel 83 ved brudd på bestemmelser i denne lovgivningen.

I personvernforordningen artikkel 83 angis vilkårene for ileggelse av gebyr. Bestemmelsen inneholder blant annet en oversikt over hvilke momenter det skal tas hensyn til, både i vurderingen av hvorvidt overtredelsesgebyr skal ilegges og i utmålingen av gebyrets størrelse.

De relevante delene av artikkel 83 nr. 1 og nr. 2 gjengis under:

> *«1. Hver tilsynsmyndighet skal sikre at ilegging av overtredelsesgebyr i henhold til denne artikkel for overtredelser av denne forordning nevnt i nr. 4, 5 og 6 i hvert enkelt tilfelle er virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende.*
>
> *2. (...) Når det treffes avgjørelse om hvorvidt det skal ilegges overtredelsesgebyr samt om overtredelsesgebyrets størrelse, skal det i hvert enkelt tilfelle tas behørig hensyn til følgende:*

a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd,
b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt,
c) eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd,
d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32,
e) eventuelle relevante tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren,
f) graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den,
g) kategoriene av personopplysninger som er berørt av overtredelsen,
h) på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen,
i) dersom tiltak nevnt i artikkel 58 nr. 2 tidligere er blitt truffet overfor den berørte behandlingsansvarlige eller databehandler med hensyn til samme saksgjenstand, at nevnte tiltak overholdes,
j) overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42 og
k) enhver annen skjerpende eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen».

Artikkel 83 angir også rammene for overtredelsesgebyrets størrelsesorden. Vi viser i denne forbindelse til artikkel 83 nr. 4 og nr. 5. De relevante delene av bestemmelsene lyder:

«4. Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges overtredelsesgebyr på opptil 10 000 000 euro (...):

a) den behandlingsansvarliges og databehandlerens forpliktelser i henhold til artikkel 8, 11, 25-39 samt 42 og 43 (...)».

«5. Ved overtredelser av følgende bestemmelser skal det i samsvar med nr. 2 ilegges overtredelsesgebyr på opptil 20 000 000 euro (...):

a) de grunnleggende prinsippene for behandling, herunder vilkår for samtykke, i henhold til artikkel 5, 6, 7 og 9,
c) overføring av personopplysninger til en mottaker i en tredjestat eller en internasjonal organisasjon i henhold til artikkel 44-49».

I personopplysningsloven § 26 første ledd fremgår det at personvernforordningen artikkel 83 nr. 4 gjelder tilsvarende for overtredelser av forordningen artikkel 24.

5. Datatilsynets vurdering

Vi viser til punkt 3 ovenfor om rekkevidden av Datatilsynets undersøkelser. I dette punkt vil vi følge samme kronologi som ovenfor.

5.1. Om personopplysninger, behandlingsansvarlig, databehandler og databehandleravtale

Datatilsynet legger til grunn at bilskilt er en personopplysning, at den manuelle billedbehandlingen av disse utgjør behandling av personopplysninger, samt at Ferde er behandlingsansvarlig og UBS er databehandler for denne behandlingen, jf. personvernforordningen artikkel 4.

Som påpekt under punkt 4.2 krever personvernforordningen artikkel 28 nr. 3 at det foreligger en databehandleravtale mellom den behandlingsansvarlige og databehandleren. Denne avtalen må være på plass *før* databehandleren kan behandle personopplysninger på vegne av den behandlingsansvarlige, nettopp fordi den pålegger både den behandlingsansvarlige og databehandleren en rekke plikter og rettigheter som må implementeres.

Datatilsynets vurdering:

Basert på beskrivelsen av de faktiske forhold under punkt 2.2 finner Datatilsynet at det er klar sannsynlighetsvekt for at Ferde ikke oppfylte plikten til å ha på plass databehandleravtale med UBS i perioden fra Ferdes overtakelse av den manuelle billedbehandlingstjenesten i september 2017 frem til september 2018. Dette er et brudd på personvernforordningen artikkel 28 nr. 3.

5.2. Risikovurdering

Som behandlingsansvarlig skulle Ferde ha gjennomført risikovurderinger før behandling av personopplysninger ble iverksatt og før den manuelle billedbehandlingen ble tatt i bruk av databehandleren. Dette for å kunne påse at opplysningene behandles med tilstrekkelig informasjonssikkerhet, jf. personvernforordningen artikkel 32.

En vurdering av risikoene forbundet med behandlingen er særlig viktig når personopplysninger overføres til land utenfor EU/EØS. I samme retning trekker omfanget av overføringen, hvorav det var estimert at det årlige behovet for manuell databehandling var knyttet til ca.10 000 000 bilder til normalbehandling og ca. 2 500 000 bilder til oppfølgingsbehandling. Uten en risikovurdering kan ikke virksomheten vurdere om risikoen er lav eller høy og dermed hvorvidt det er nødvendig med ytterligere sikkerhetstiltak.

Datatilsynets vurdering:

Etter Datatilsynets oppfatning, som baserer seg på de faktiske forhold som beskrevet under punkt 2.3, er det klar sannsynlighetsvekt for at Ferde manglet skriftlig risikovurdering i perioden fra Ferdes overtakelse av den manuelle billedbehandlingstjenesten i september 2017 frem til oktober 2019. Dette utgjør et brudd på personvernforordningen artikkel 32 nr. 2, jf. artikkel 5 nr. 1 bokstav f og artikkel 5 nr. 2.

5.3. Overføring av personopplysninger utenfor EØS/EU

Overføring av personopplysninger utenfor EØS/EU krever blant annet grunnlag for overføringen i tråd med personvernforordningen kapittel 5, jf. artikkel 44.

Datatilsynets vurdering:

Basert på beskrivelsen av de faktiske forhold under punkt 2.4 finner Datatilsynet at det foreligger klar sannsynlighetsvekt for at Ferde ikke hadde grunnlag for overføring av personopplysninger til Kina i perioden september 2017 frem til våren 2019. Dette er et brudd på personvernforordningen artikkel 44. Basert på den tilgjengelige informasjonen, kan Datatilsynet ikke se at unntakene i artikkel 49 kom til anvendelse i ovennevnte tidsperiode.

6. Overtredelsesgebyr

6.1. Vurdering av om overtredelsesgebyr skal ilegges

Overtredelsesgebyr er et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsregelverket. Vi mener det er nødvendig å reagere på overtredelsene, og ilegger med dette overtredelsesgebyr (jf. personvernforordningen artikkel 83).

I samsvar med Høyesteretts praksis (jf. Rt. 2012 side 1556) legger vi til grunn at overtredelsesgebyr er å anse som straff etter den europeiske menneskerettighetskonvensjonen artikkel 6. Det kreves derfor klar sannsynlighetsovervekt for lovbrudd for å kunne ilegge gebyr. I sitt brev til Datatilsynet den 20. mai 2021 erkjenner Ferde at det er skjedd brudd på personopplysningsloven, som gjør personvernforordningen til norsk rett. Selskapet mener imidlertid at gebyrutmålingen er for høy, og at det endelige gebyret bør være vesentlig lavere.

Datatilsynet kan ilegge overtredelsesgebyr etter en skjønnsmessig helhetsvurdering. Ved vurderingen og utmålingen skal det tas hensyn til momentene i personvernforordningen artikkel 83 nr. 2 a) til k).

Vi vil her vurdere de relevante momentene fortløpende.

a) karakteren, alvorlighetsgraden og varigheten av overtredelsen, idet det tas hensyn til den berørte behandlingens art, omfang eller formål samt antall registrerte som er berørt, og omfanget av den skade de har lidd

Overtredelsen innebærer brudd på de grunnleggende kravene om å ha på plass databehandleravtale, risikovurdering for å sikre tilstrekkelig sikkerhet ved behandlingen samt overføringsgrunnlag ved overføring av personopplysninger utenfor EU/EØS. Dette må karakteriseres som et klart avvik fra de pliktene som følger av personvernforordningen, og disse forholdene vurderer Datatilsynet som svært skjerpende omstendigheter.

Personopplysningene som saken gjelder er bilskilt. Sammen med bilskiltet ligger det informasjon om passeringstidspunkt, samt en numerisk kode for hvilken stasjon som er passert. Øvrige deler av bilen er sladdet, slik at fører ikke identifiseres.

Ferde anfører i brev av 20. mai 2021 at selv om det er kritikkverdig at personopplysningene i denne sak er overført til tredjestat, tilsier opplysningskategorien at det neppe er nødvendig å reagere så strengt som foreslått i varselet. Dette fordi det verken er snakk om særlige kategorier av personopplysninger eller opplysninger om straffbare forhold mv. I tillegg

anfører Ferde at selskapet ikke kan se at en risikovurdering her ville tilsagt at skadepotensialet er betydelig.

Datatilsynet kan ikke se at disse er nye argumenter. Selv om det skulle vise seg at håndteringen av personopplysningene ikke anses som særlig risikofylt, er poenget at man ikke kjenner den konkrete risikoen før man har gjennomført en risikovurdering. Det kan være enkelt å finne personer når man har tilgang til bilder av skilter og bilnummer. Dersom det oppstår en hendelse som gir operatørene i Kina større adgang til informasjon enn forutsatt, kan det være mulig å finne ut av hvilke personer som har befunnet seg på hvilke steder i bompengeregionen. Uten en databehandleravtale og overføringsgrunnlag har man heller ikke sikret at databehandler behandler personopplysningene de får tilgang til, på en tilfredsstillende måte. Personvernforordningen krever en databehandleravtale, risikovurdering samt overføringsgrunnlag for å angi rammene for håndteringen av opplysningene samt på forhånd avdekke mulige svakheter i det manuelle billedbehandlingssystemet og sørge for sikker og konfidensiell behandling av personopplysninger. Dette er viktig for å minimere risikoen for misbruk mv. knyttet til behandlingen. Det kan også fremheves at størrelsen på gebyret hadde vært betraktelig høyere dersom det hadde vært snakk om overføring av særlige kategorier med personopplysninger eller opplysninger om straffbare forhold mv.

Ferde estimerte, med utgangspunkt i historiske data, at det årlige behovet for manuell databehandling ville være ca. 10 000 000 bilder til normalbehandling og 2 500 000 bilder til oppfølgingsbehandling. Mengden med personopplysninger som blir overført til Kina må anses som betydelig, og Datatilsynet anser dette som en skjerpende omstendighet.

Basert på tilgjengelig informasjon foreligger det ingen indikasjon på at personopplysningene til bilførerne har kommet på avveie. Det er dermed ikke klar sannsynlighetsovervekt for materiell eller ikke-materiell skade lidt av de registrerte. At det ikke kan påvises noen slik konkret skade lidt er en formildende omstendighet i saken.

Datatilsynet finner at det foreligger klar sannsynlighetsvekt for at Ferde manglet databehandleravtale, risikovurdering og overføringsgrunnlag i en betydelig periode (mellom ca. 1-2 år), mens den aktuelle behandlingen av personopplysninger fant sted. Varigheten av overtredelsen anses derfor som en skjerpende omstendighet.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Det fremgår av Høyesterettsdom HR-2021-797-A at ved ileggelse av foretaksstraff så stilles krav om at den som har opptrådt på vegne av foretaket i hvert fall har utvist alminnelig uaktsomhet. Vi legger til grunn at det samme gjelder for ileggelse av overtredelsesgebyr som administrativ sanksjon overfor foretak basert på tidligere nevnt rettspraksis.

Den aktuelle behandlingen av personopplysninger ble gjennomført uten at det forelå databehandleravtale, risikovurderinger eller overføringsgrunnlag for overføring av personopplysninger til Kina. Datatilsynet anser at dette må karakteriseres som klart uaktsomt å ikke ha på plass disse sentrale instrumentene etter personvernregelverket og Ferde som behandlingsansvarlig har ansvar for å sørge for at alle plikter etter personvernforordningen er

oppfylt jf. personvernforordningen artikkel 5 nr. 2 (ansvarlighetsprinsippet). Videre legger vi til grunn at ansvaret ligger hos styret i Ferde AS, jf. aksjeloven § 6-12 første ledd første punktum og aksjeloven § 6-30. Vi understreker styrets tilsynsansvar med selskapets virksomhet jf. aksjeloven § 6-13. Denne uaktsomheten tillegges styret ved styreleder som må anses som å ha opptrådt på vegne av selskapet.

c) *eventuelle tiltak truffet av den behandlingsansvarlige eller databehandleren for å begrense skaden som de registrerte har lidd*

Ferde fikk etterhvert på plass databehandleravtale, risikovurdering, samt overføringsgrunnlag etter personvernforordningen kapittel 5. Dette er imidlertid ikke et moment som er relevant i saken.

d) *den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32*

Det faktum at den aktuelle behandlingen av personopplysninger ble gjennomført uten at det forelå databehandleravtale, risikovurderinger eller overføringsgrunnlag etter personvernforordningen kapittel 5, gir uttrykk for alvorlige mangler ved det interne styringssystemet. Plikten til å ha på plass disse instrumentene er sentrale etter personvernforordningen. Dette trekker i retning av et overtredelsesgebyr.

e) *eventuelle tidligere overtredelser begått av den behandlingsansvarlige eller databehandleren*

Datatilsynet har ikke vektlagt noen tidligere overtredelser i denne saken.

f) *graden av samarbeid med tilsynsmyndigheten for å bøte på overtredelsen og redusere de mulige negative virkningene av den*

Ferde har svart på spørsmålene fra Datatilsynet slik de er påkrevd. Dette trekker derfor hverken i skjerpende eller formildende retning.

g) *kategoriene av personopplysninger som er berørt av overtredelsen*

Se ovenfor under a)

h) *på hvilken måte tilsynsmyndigheten fikk kjennskap til overtredelsen, særlig om og eventuelt i hvilken grad den behandlingsansvarlige eller databehandleren har underrettet om overtredelsen*

Datatilsynet ble kjent med overtredelsen gjennom nyhetsartikler publisert av NRK, og mer spesifikt gjennom Kluges rapport. Dette trekker hverken i skjerpende eller formildende retning.

i) dersom tiltak nevnt i artikkel 58 nr. 2 tidligere er blitt truffet overfor den berørte behandlingsansvarlige eller databehandler med hensyn til samme saksgjenstand, at nevnte tiltak overholdes

Det er ikke tidligere truffet tiltak overfor Ferde med hensyn til samme saksgjenstand.

j) overholdelse av godkjente atferdsnormer i henhold til artikkel 40 eller godkjente sertifiseringsmekanismer i henhold til artikkel 42

Datatilsynet finner ikke dette momentet relevant i saken.

k) og enhver annen skjerpende eller formildende faktor ved saken, f.eks. økonomiske fordeler som er oppnådd, eller tap som er unngått, direkte eller indirekte, som følge av overtredelsen

Datatilsynet har ikke informasjon som tilsier at Ferde har oppnådd særlige økonomiske fordeler ved saken, annet enn å få alminnelige driftsinntekter gjennom å kreve inn bompenger. Datatilsynet legger derfor til grunn at Ferde ikke har oppnådd noen økonomiske fordeler som følge av overtredelsen. Dette trekker derfor hverken i skjerpende eller formildende retning.

Datatilsynet har ikke vurdert eller avdekket at manglende databehandleravtale, risikovurdering eller overføringsgrunnlag har medført konsekvenser for behandlingen av personopplysninger, herunder påvirket rettighetene og frihetene til de registrerte. Datatilsynet har ikke kjennskap til andre skjerpende eller formildende faktorer ved saken som vil påvirke utfallet av vurderingen.

Datatilsynet er etter dette kommet til at overtredelsesgebyr bør ilegges, jf. personvernforordningen artikkel 83 nr. 2, 4 og 5.

6.2. Vurdering av gebyrets størrelse

Overtredelsesgebyret skal i henhold til artikkel 83 nr. 1 være virkningsfullt, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Dette innebærer at tilsynsmyndigheten skal gjøre en konkret, skjønnsmessig vurdering i hvert enkelt tilfelle.

Ved utmåling av gebyrets størrelse skal det legges vekt på de samme vurderingsmomentene som er gjennomgått i vedtakets punkt 6.1. Datatilsynet viser derfor til vurderingene gjort ovenfor, og at disse samlet taler for et gebyr av en viss størrelse.

Ferde anfører i sitt brev av 20. mai 2021 at Datatilsynet bør ta sakens forhistorie i betraktning ved gebyrutmålingen. Ferde påpeker at avtalen med UBS ikke var fremhevet som et forhold av betydning i forbindelse med selskapsgjennomgangen i oppkjøpsprosessen og at forholdene på overdragelsestidspunktet var ukjente. Datatilsynet kan ikke se at dette momentet bør spille inn på vurderingen av gebyret størrelse. Nettopp det at virksomhetsoverdragelsen var stor og komplisert taler for at behovet for dokumentasjon og avdekking av risiko er høyere og burde blitt nøye vurdert i selskapsgjennomgangen.

Datatilsynet er uenig i relevansen av momentet som Ferde trekker frem i sitt brev av 20. mai 2021 om at tidspunktet for rettsbruddet bør gjenspeiles i utmålingen. Vi vil derfor ikke vektlegge det ved utmålingen.

Datatilsynet kan heller ikke se at sakene som Ferde referer til i brev av 20. mai 2021 er sammenlignbare med foreliggende sak. PVN-2015-04 gjaldt, som Ferde påpeker, brudd etter personopplysningsloven 2000 hvor gebyrstørrelsen var lavere. I tillegg gjaldt den saken kun manglende databehandleravtale, mens foreliggende sak gjelder flere forhold.

Én sak vi imidlertid anser som noenlunde sammenlignbar er en nyere avgjørelse fra det spanske datatilsynet, hvor de ila Vodafone Spania et overtredelsesgebyr på mer enn 8 millioner euro for brudd på personvernforordningen artikkel 28 og 44.[8]

I skjerpende retning legger vi særlig vekt på Ferdes klare avvik fra de sentrale pliktene som personvernforordningens artikkel 28 nr. 3, artikkel 32 nr. 2, jf. artikkel 5 nr. 1 bokstav f og artikkel 5. nr. 2, og artikkel 44 oppstiller. Vi vektlegger også særlig omfanget av personopplysninger som er berørt av overtredelsen, og spesielt at personopplysninger er overført til land utenfor EU/EØS.

I formidlende retning legger vi vekt på at det ikke er kjent eller klar sannsynlighetsovervekt for at bruddet har ført til materiell eller ikke-materiell skade for de registrerte som er berørt.

Også virksomhetens økonomiske evne vil være av betydning, selv om det ikke er aktuelt å utnytte det spennet i overtredelsesgebyrets størrelse som følger av artikkel 83. nr. 5. Personvernforordningen artikkel 83 nr. 5. fastsetter et høyere maksbeløp for gebyr når saken omhandler overtredelser av de grunnleggende prinsippene for behandling av personopplysninger i henhold til personvernforordningen artikkel 5 og 6.

Ifølge Ferdes regnskap fra 2019 hadde Ferde driftsinntekter på 3 553 242 352 kroner, driftskostnader på 303 148 828 kroner og en gjeld på 22 830 821 738 kroner.[9] Driftsinntektene stammer fra hovedsakelig fra passeringsinntekter og delvis fra statlig tilskudd og andre inntekter. Datatilsynet har ikke funnet regnskapstall fra 2020, men legger til grunn at tallene fra 2019 er noenlunde tilsvarende som tallene for 2020.

Datatilsynet er uenig i Ferde sin anførsel som fremgår av brev 20. mai 2021 om at det er relevant å se på tall lengre tilbake. Ferde viser i den sammenheng til EU-domstolens avgjørelse Case C-76/06 P av 7. juni 2007. Datatilsynet mener at det ikke er relevant å vise til denne avgjørelsen, da saksforholdet var spesielt fordi det ikke var noen omsetning året før å ta utgangspunkt i.

Ferdes betydelige økonomiske tall taler for at vedtaket må være av en viss størrelse for at de preventive hensynene bak overtredelsesgebyr som reaksjonsform skal ivaretas.

---

[8] EDPB: "Spanish DPA Fines Vodafone Spain more than 8 Million Euros", 31. mars 2021. https://edpb.europa.eu/news/national-news/2021/spanish-dpa-fines-vodafone-spain-more-8-million-euros_en, sist åpnet 8. juli 2021.

[9] Ferdes årsberetning 2019: https://issuu.com/hg-9/docs/ferde_aarsmelding_2019?fr=sYjM5ZDExNTUzNTQ

Etter en helhetsvurdering av momentene i saken som vi har gjennomgått ovenfor og alvorligheten i overtredelsen, har vi kommet frem til at et overtredelsesgebyr på kr 5 000 000 anses riktig.

7. Oppfyllelsesfrist og klageadgang

Dere kan klage på vedtaket. En eventuell klage må sendes til Datatilsynet innen tre uker etter at dette brevet er mottatt, jf. forvaltningsloven §§ 28 og 29. Dersom vi opprettholder vårt vedtak, vil vi sende saken til Personvernnemnda for klagebehandling jf. personopplysningsloven § 22.

Dersom dere ikke påklager pålegget om overtredelsesgebyr, er oppfyllelsesfristen fire uker etter klagefristens utløp, jf. personopplysningsloven § 27.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Tanja Czelusniak
juridisk rådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer