Datatilsynet

STATENS VEGVESEN
Postboks 8142 Dep
0033 OSLO

Deres referanse	Vår referanse	Dato
	18/04147-23/KBK	25.02.2020

Varsel om vedtak om pålegg og overtredelsesgebyr

1. Innledning

Vi viser til klage fra Ole Østlid av 10. desember 2018 **(18/4147 – 1)**, korrespondanse mellom Fjellinjen AS («Fjellinjen») og Statens vegvesen (SVV) **(18/4147 – 7 og 8)**, Q-Free's redegjørelse til Datatilsynet **(18/4147 – 13)** vedrørende ansvarsforhold til systemet samt øvrig korrespondanse i saken.

Saken gjelder manglende sletting av passeringsopplysninger i bomringen. Saken blir redegjort nærmere under pkt. 3.

2. Lovovertredelsen

Den manglende slettingen av passeringsopplysninger i bomringen innebærer forhold som utgjør mulige brudd på personvernforordningen artikkel 5 nr. 1, artikkel 17 nr. 1. og artikkel 25. nr.1. Dette gjelder:

- Lagring av passeringsopplysninger utover den tid SVV lovlig kan oppbevare disse, er et brudd på personvernforordningen artikkel 5 nr. 1 bokstav a), og artikkel 17 nr. 1 bokstav a) og d).

- Manglende implementering av passende tekniske og organisatoriske tiltak som er utformet for å implementere personvernprinsippene, for eksempel dataminimering, på en effektiv måte og å integrere de nødvendige sikkerhetstiltakene i behandlingene for å oppfylle kravene i personvernforordningen og beskytte de registrertes rettigheter, jf. artikkel 25 nr. 1, jf. artikkel 5 nr. 1, bokstav c), d), e) og f).

3. Varsel om vedtak om pålegg og overtredelsesgebyr

3.1 Varsel om pålegg – art. 58 nr. 2 bokstav d)

Dette er et varsel om at Datatilsynet, med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav d), jf. forvaltningsloven § 16, vurderer å fatte vedtak om følgende pålegg:

1) *Statens vegvesen må, uten ugrunnet opphold, slette personopplysninger om brikkenummer, lokasjon og passeringstidspunkt som lagres utover den tid virksomheten*

lovlig kan oppbevare disse personopplysningene, da personopplysningene ikke lenger er nødvendige for formålet som de ble samlet inn eller behandlet for, jf. personvernforordningen artikkel 17 nr. 1 bokstav a) og d), jf. artikkel 5 nr. 1 bokstav a), c), d), e) og f).

2) *Statens vegvesen må, uten ugrunnet opphold, slette personopplysninger som lagres om klager utover den tid virksomheten lovlig kan oppbevare disse, jf. personvernforordningen artikkel 17 nr. 1 bokstav a), jf. artikkel 5 nr. 1 bokstav a) og c).*

Varselet om pålegg er nærmere begrunnet under pkt. 6.2.

3.2 Varsel om overtredelsesgebyr – artikkel 58 nr. 2 bokstav i)
I medhold av personopplysningsloven § 26 andre ledd kan Datatilsynet ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 58 nr. 2 bokstav i), jf. artikkel 83 nr. 7.

Dette er et varsel etter forvaltningsloven § 16 om at Datatilsynet vil vurdere å fatte følgende vedtak om overtredelsesgebyr:

- *Statens vegvesen pålegges i medhold av personopplysningsloven § 26 andre ledd, jf. personvernforordningen artikkel 83, å betale et overtredelsesgebyr til statskassen på **4 000 000** – fire millioner – kroner for å ikke ha slettet passeringsopplysninger om brikkenummer, lokasjon og passeringstidspunkt som lagres utover den tid SVV lovlig kan oppbevare disse, jf. artikkel 17 nr. 1 bokstav a) og d), jf. artikkel 5 nr. 1 bokstav a), og for ikke å ha implementert passende tekniske og organisatoriske tiltak som er utformet for å implementere personvernprinsippene, for eksempel dataminimering, på en effektiv måte og å integrere de nødvendige sikkerhetstiltakene i behandlingene for å oppfylle kravene i personvernforordningen og beskytte de registrertes rettigheter, jf. artikkel 25 nr. 1, jf. artikkel 5 nr. 1, bokstav c), d), e) og f).*

Varselet om overtredelsesgebyr er nærmere begrunnet under pkt. 6.3.

4. Sakens faktiske forhold
Saken er initiert i en klage fra en privatperson, som påpekte at Fjellinjen lagret passeringsinformasjon som var eldre enn fem år. Passeringsinformasjon omfatter alle passeringer som kjøretøy foretar gjennom bomringen, inkludert opplysninger om bilens brikkenummer (koblet til registreringsnummer), lokasjon og passeringstidspunkt. I tilsvaret til klager, opplyste Fjellinjen at selskapet var pliktig til å oppbevare passeringsdata i fem år i henhold til bokføringsreglene. Klager har i klagen sannsynliggjort at det lagres passeringsdata som er eldre enn fem år, og at Fjellinjen også har registrert og lagret opplysninger om klagers bosted tilbake til 2008 og 2010. Klager har bedt om at disse opplysningene blir slettet.

Systemet hvor personopplysninger om kjøretøy som passerer bompengeringen og tilhørende fakturaer lagres, heter CS Norge. SVV og Fjellinjen har inngått en avtale om felles behandlingsansvar for den behandlingen av personopplysninger som skjer i dette systemet.

SVV og Fjellinjen har også avtalt å utveksle personopplysninger i systemet seg imellom. Lignende avtaler er inngått mellom SVV og de øvrige bompengeselskapene.

SVV har pålagt alle bompengeselskapene i Norge å bruke dette systemet, som leveres av Q-Free ASA. Det er SVV som er systemeier og ansvarlig for applikasjonens funksjonalitet. Det er SVV som bestemmer formålet med behandlingen og midlene for behandlingen, jf. personvernforordningen artikkel 4 nr. 7. SVV har utarbeidet en spesifikasjon for endring av systemet, slik at oppbevaringskravene i personvernforordningen skulle ivaretas. SVV sendte oppdragsbestillingen til Q-Free 22. mars 2018. I brev av 12. april 2019 til SVV opplyste Fjellinjen at det ikke finnes funksjonalitet som gjør at Fjellinjen kan utføre sletting på angitt kunde.

I brev av 23. mai 2019 til SVV uttaler Fjellinjen at Fjellinjen ikke kan *«effektuere de endringer som systemteknisk er nødvendig å utføre i CS Norge. Selv om SVV som Fjellinjen har såkalt «delt behandleransvar» er systemeierskapet uomtvistelig SVV via avtale med Q-Free as.*

Fjellinjen har kontaktet Q-Free der det oppgis at forholdet er kjent for SVV. Q-Free har utarbeidet løsningsforslag og gjennom siste halvår purret SVV i sakens anledning og sist før påske.»

Fjellinjen uttaler videre i samme brev til SVV:

«Fjellinjen tar i betraktning at Q-Free som leverandør av basissystemet for AutoPass har et selvstendig ansvar for å være i overensstemmelse med GDPR. Dette kan likevel ikke være årsak til at SVV som systemansvarlig lar være å rekvirere endringer som er nødvendig for at Bomselskapene kan ivareta lovverket ovenfor kunden som for eget selskap».

I sitt svar til Fjellinjen av 31. mai 2019, uttaler SVV at SVV *«allerede 23. mars 2018 meldte inn en oppdragsbestilling til Q-Free for å få slettet data. Etter bestillingen har det bl.a. oppstått diskusjoner/uenigheter mellom partene, der Statens vegvesen mener Q-Free i det vesentlige har bidratt til forsinkelsene i prosessen med å få på plass en slettefunksjon som ivaretar kravene etter personvernregelverket på best mulig måte.»* Det heter videre at det blir *«uriktig å fremstille det slik at Q-Free har purret på i et halvår, mens Statens vegvesen har «latt være» å gjennomføre de endringer som er nødvendig for regeletterlevelse. Slettesaken med Q-Free er stor og komplisert. Den baserer seg på et omfattende avtaleverk og kompliserte tekniske forhold.»*

I brev av 24. juni 2019 gir Q-Free en tilbakemelding til SVV, hvor selskapet påpeker at SVV gir feilaktige opplysninger i sitt brev av 31. mai 2019:

«I mai 2017 initierer Q-Free diskusjoner med SVV om GDPR. SVV utsetter diskusjonen til over sommeren for beholde fokus på planlagt implementasjon av ny MinSide & IF-adapter.

I august 2017 hyrer SVV inn Eva Jarbekk for å skrive en utredning om nye personvernregler som QFree skulle få innsyn i. Det får vi aldri. I januar 2018 påpeker Q-Free i et

styringsgruppemøte med SVV at vi ikke har fått innsyn i Jarbekks rapport. Vi ber om at GDPR blir et fast agendapunkt i fremtidige styringsgruppemøter.

I mars 2018 kommer det en oppdragsbestilling fra SVV til Q-Free for å få slettet persondata som SVV ikke har hjemmel for å lagre ihht de nye GDPR-reglene (krav om «engangssletting»). SVVs bestilling krever ifølge Q-Free tekniske endringer i systemet, men SVV tilbakeviser dette til tross for at Q-Free dokumenterer sitt syn i et 25-siders notat som deles med SVV i mai 2018.

I mai 2018 ber SVV Q-Free om å signere ny databehandleravtale hvor Q-Free skal bekrefte at CS Norge oppfyller alle kravene i GDPR. Dette avviser Q-Free på bakgrunn av at det ikke er utstedt en formell endringsordre fra SVV med planlagte tiltak for å lukke avvik som gjør at CS Norge kan oppfylle GDPR-kravene.

I slutten av mai 2018 distribuerer Q-Free et nytt notat til SVV som kartlegger områder i CS Norge som potensielt krever endringer ifm innføring av GDPR. Dette er et resultat av en lengre GAP-utredning fra Q-Free og som benyttes som grunnlag for videre diskusjoner med SVV.

28. juni 2018 deler Q-Free et teknisk løsningsforslag med SVV som tar høyde for de aspekter som har fremkommet etter omfattende diskusjoner mellom partene og som i utgangspunktet avslutter SVVs oppdragsbestilling og kravet om «engangssletting».

29. august 2018 sender Q-Free et brev til SVVs personvernombud der vi som databahandler informerer behandlingsansvarlig om kjente avvik i forhold til ny personopplysningslov/ GDPR. Umiddelbar tilbakemelding fra SVV er at saken blir håndtert videre av prosjektleder for CS Norge i SVV. 19. september 2018, etter purring fra Q-Free den 12. september 2018, mottar Q-Free en epost fra SVVs personvernombud der det vises til pågående samtaler om databehandleravtale og det informeres om at saken er videresendt til seksjonen for brukerfinansiering og at videre oppfølging vil skje via dem.

Tidlig i september 2018 blir et fakturaforslag med bl.a. 200 timer for GDPR-arbeid oversendt SVV. Dette avvises fordi bruk av timer på GDPR ikke er formelt avklart.

Frem mot jul 2018 avholdes det en rekke møter mellom Q-Free og SVV, der jurister også er involvert, for å avklare hvem som skal dekke kostnadene for GDPR-tilpasninger. Partene blir ikke enige.

I desember 2018 oppretter SVV på nytt en oppdragsbestilling hvor man opprettholder kravet om «engangssletting».

I januar 2019 foreslår Q-Free at man deler kostnadene 50/50 for å komme videre. SVV aksepterer dette forslaget senere samme måned. SVV aksepterer dessuten at sletting av data krever endring i funksjonaliteten i CS Norge. Endringsordre på sletting etableres av SVV slik at Q-Free endelig kan ferdigstille et formelt løsningsforslag.

I perioden februar-april 2019 avholdes det en rekke arbeidsmøter mellom partene. SVV krever at enkelte problemstillinger diskuteres med SVVs revisor. Dette arbeidet tar tid fordi revisor skal konferere med skattedirektoratet og andre underveis. Løsningsbeskrivelsen kan ikke ferdigstilles før revisors tilbakemeldinger er implementert, men endelig tilbakemelding fra revisor kommer ikke før i april.

12.april 2019 distribuerer Q-Free et løsningsforslag etter avklaringer med SVVs revisor. Avtalt Prosess var at SVV skulle godkjenne det tekniske løsningsforslaget, og at Q-Free så skulle lage et formelt tilbud basert på dette. Etter påske har Q-Free gjentatte ganger purret SVV om en tilbakemelding inkl. i styringsgruppemøter. Vi venter fortsatt, over 2 måneder etter at forslaget ble sendt.»

8. juni 2019 ble det avholdt et møte mellom SVV og Datatilsynet, hvor SVV informerte Datatilsynet om prosessen med sletting av personopplysninger i CS Norge. SVV har etter dette informert Datatilsynet løpende om utviklingen i saken. Parallelt med SVVs arbeid med å forbedre personvernet i gjeldende systemløsninger, jobber SVV også med å etablere nye systemløsninger på bompengeområdet.

Klager har ennå ikke fått sitt krav om sletting effektuert.

5. Regelverket på området

5.1 Reglene i personvernforordningen

Personvernforordningen artikkel 5 gir uttrykk for kjernen i personvernretten. Overtredelse av prinsippene i art. 5 kan i seg selv føre til ileggelse av sanksjoner. Det følger for eksempel av art. 83 nr. 5 at overtredelser av art. 5 er blant de lovovertredelsene som kan resultere i de høyeste overtredelsesgebyrene. Maksimumsbeløpet er 20 000 000 euro, p.t. ca. 200 millioner NOK, for behandlingsansvarlige eller databehandlere som ikke er foretak, jf. også personopplysningsloven § 26 andre ledd.

De aktuelle rettsreglene på området er:

> **Artikkel 5.** ***Prinsipper for behandling av personopplysninger***
>
> 1. Personopplysninger skal
> a) behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),
>
> b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenlig med disse formålene; viderebehandling for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål skal, i samsvar med artikkel 89 nr. 1, ikke anses som uforenlig med de opprinnelige formålene («formålsbegrensning»),
>
> c) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»),

d) være korrekte og om nødvendig oppdaterte; det må treffes ethvert rimelig tiltak for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold slettes eller rettes («riktighet»),

e) lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig for formålene som personopplysningene behandles for; personopplysninger kan lagres i lengre perioder dersom de utelukkende vil bli behandlet for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål i samsvar med artikkel 89 nr. 1, forutsatt at det gjennomføres egnede tekniske og organisatoriske tiltak som kreves i henhold til denne forordning for å sikre de registrertes rettigheter og friheter («lagringsbegrensning»),

f) 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 («integritet og konfidensialitet»).

2. Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at nr. 1 overholdes («ansvar»).

Artikkel 6. ***Behandlingens lovlighet***

1. Behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:

a) den registrerte har samtykket til behandling av sine personopplysninger for ett eller flere spesifikke formål,

b) behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,

c) behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige,

d) behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons vitale interesser,

e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,

f) behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.

Nr. 1 bokstav f) får ikke anvendelse på behandling som utføres av offentlige myndigheter som ledd i utførelsen av deres oppgaver.

Artikkel 17. ***Rett til sletting («rett til å bli glemt»)***

1. Den registrerte skal ha rett til å få personopplysninger om seg selv slettet av den behandlingsansvarlige uten ugrunnet opphold, og den behandlingsansvarlige skal ha plikt til å slette personopplysninger uten ugrunnet opphold dersom et av de følgende forhold gjør seg gjeldende:

a) personopplysningene er ikke lenger nødvendige for formålet som de ble samlet inn eller behandlet for,

b) den registrerte trekker tilbake samtykket som ligger til grunn for behandlingen, i henhold til artikkel 6 nr. 1 bokstav a) eller artikkel 9 nr. 2 bokstav a), og det ikke finnes noe annet rettslig grunnlag for behandlingen,

c) den registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 1, og det ikke finnes mer tungtveiende berettigede grunner til behandlingen, eller den registrerte protesterer mot behandlingen i henhold til artikkel 21 nr. 2,

d) personopplysningene er blitt behandlet ulovlig,

e) personopplysningene må slettes for å oppfylle en rettslig forpliktelse i unionsretten eller medlemsstatenes nasjonale rett som den behandlingsansvarlige er underlagt,

f) personopplysningene er blitt samlet inn i forbindelse med tilbud om informasjonssamfunnstjenester som nevnt i artikkel 8 nr. 1.

Artikkel 25. ***Innebygd personvern og personvern som standardinnstilling***

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, skal den behandlingsansvarlige, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.

2. Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles. Nevnte forpliktelse får anvendelse på den mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet. Nevnte tiltak skal særlig sikre at personopplysninger som standard ikke gjøres tilgjengelige for et ubegrenset antall fysiske personer uten den berørte personens medvirkning.

3. En godkjent sertifiseringsmekanisme i henhold til artikkel 42 kan brukes som en faktor for å påvise at kravene fastsatt i nr. 1 og 2 i denne artikkel overholdes.

Artikkel 26. ***Felles behandlingsansvarlige***

1. Dersom to eller flere behandlingsansvarlige i fellesskap fastsetter formålene med og midlene for behandlingen, skal de være felles behandlingsansvarlige. De skal på en åpen måte fastsette sitt respektive ansvar for å overholde forpliktelsene i denne forordning, særlig med hensyn til utøvelse av den registrertes rettigheter og den plikt de har til å framlegge informasjonen nevnt i artikkel 13 og 14, ved hjelp av en ordning seg imellom, med mindre og i den grad de behandlingsansvarliges respektive ansvar er fastsatt i unionsretten eller medlemsstatenes nasjonale rett som de behandlingsansvarlige er underlagt. I ordningen kan det utpekes et kontaktpunkt for registrerte.

2. Ordningen nevnt i nr. 1 skal på behørig måte gjenspeile de felles behandlingsansvarliges respektive roller og forhold til de registrerte. Det vesentligste innholdet i ordningen skal gjøres tilgjengelig for den registrerte.

3. Uavhengig av vilkårene for ordningen nevnt i nr. 1 kan den registrerte utøve sine rettigheter i henhold til denne forordning med hensyn til og overfor hver av de behandlingsansvarlige.

5.2 Særlig om ileggelse av overtredelsesgebyr – artikkel 58 nr. 2 bokstav i

Personvernforordningen overlater til medlemsstatene å fastsette om overtredelsesgebyr skal kunne ilegges offentlige myndigheter og organer, jf. artikkel 83 nr. 7. I personopplysnings-loven § 26 andre ledd er det bestemt at Datatilsynet kan ilegge offentlige myndigheter og organer overtredelsesgebyr etter reglene i personvernforordningen artikkel 58, jf. artikkel 83 nr. 7.

6. Datatilsynets begrunnelse for å fatte vedtak

6.1 Behandlingsansvaret

SVV og Fjellinjen har felles behandlingsansvar for de behandlingene av personopplysninger som er omtalt ovenfor. Etter personvernforordningen artikkel 26 nr. 1 skal to eller flere behandlingsansvarlige være felles behandlingsansvarlige når de i fellesskap fastsetter formålet og midlene med behandlingen. Det er videre et krav at de skal fastsette sitt respektive ansvar for å overholde forpliktelsene i forordningen. Dette skal skje på en åpen måte.

Det er, slik Datatilsynet ser det, myndighetene som fastsetter formålet med bruken av bomstasjoner. Fjellinjen har liten innflytelse på dette. Likeledes er det SVV som er systemeier, og det er SVV som inngår kontrakt med leverandøren om hvilket system som skal brukes, og det er dermed SVV som bestemmer hvilke «midler som skal benyttes», jf. personvernforordningen artikkel 4 nr. 7. Fjellinjen har ikke hatt noen direkte innflytelse på de

forhold som tas opp i dette varselet, og Fjellinjen kan følgelig ikke sies å ha noe behandlingsansvar for de aktuelle personopplysningene. SVV må således regnes som behandlingsansvarlig for de behandlinger av personopplysninger som er aktuelle i denne saken.

6.2 Pålegg om iverksetting av tiltak

6.2.1 Ulovlig lagring av passeringsopplysninger i bomringen

SVV kan bare lovlig behandle personopplysninger ved passeringer i bomringen når det er behandlingsgrunnlag for dette, jf. personvernforordningen artikkel 6. Er behandlingen av personopplysninger ulovlig, så skal personopplysningene slettes, jf. artikkel 17 nr. 1 bokstav d). I utgangspunktet lagres personopplysninger for passering i bomringen som fakturagrunnlag, og har behandlingsgrunnlag i artikkel 6 nr. 1 bokstav b). Fakturagrunnlaget vil da bli slettet når kunden har gjort opp for seg. Imidlertid er det et krav etter bokføringsloven § 13 at primærdokumentasjon skal oppbevares i inntil 5 år etter regnskapsårets slutt. Lagring av passeringsopplysninger i bompengesystemet utover dette tidspunkt skal slettes uten ugrunnet opphold, jf. artikkel 17 nr. 1.

Dernest kan det konstateres at det vil være et brudd på artikkel 17 nr. 1 bokstav a) hvis personopplysninger ved passeringer i bomringen oppbevares lenger enn hva kravet etter bokføringsloven er. Da tilfredsstiller ikke lagringen av opplysningene nødvendighetskravet i bestemmelsen, og skal da slettes.

6.2.2 Innebygd personvern og personvern som standardinnstilling

Det opprinnelige systemet for lagring av passeringsopplysninger kunne ikke funksjonelt slette personopplysninger om passeringer i bomringen. Det har i løsningen ikke blitt vurdert å gjennomføre egnede tekniske og organisatoriske tiltak for å oppfylle kravene i personvernforordningen og beskytte de registrertes rettigheter. Det vil være et brudd på artikkel 25 nr. 1 bokstav d), jf. artikkel 5 nr. 1 bokstav c), d) e) og f) at man ikke har gjennomført tiltak for innebygd personvern eller personvern som standardinnstilling.

6.2.3 Ulovlig lagring av passeringsopplysninger om klager

Saken er initiert på bakgrunn av en klage. At sletting ikke kunne gjennomføres på vedkommende er ikke forenlig med de grunnleggende rettigheter klager har etter personvernforordningen artikkel 17 nr. 1 bokstav a), c) og d), jf. artikkel 5 nr. 1 bokstav a).Klager har protestert på lagringen. Det kan således konstateres et brudd på artikkel 17 nr. 1 bokstav c), da det ikke kan godtgjøres at lagringen skjer på grunn av «mer tungtveiende berettigede grunner», se artikkel 21 nr. 1.

6.3 Datatilsynets vurdering av vedtaket om overtredelsesgebyr

Adgangen til å ilegge overtredelsesgebyr er gitt som et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsloven. Internrettslig er overtredelsesgebyr ikke å anse som en straff, men en administrativ sanksjon. Det må imidlertid antas at overtredelsesgebyr er å anse som straff etter EMK (Den europeiske menneskerettskonvensjonen) artikkel 6, og i samsvar med Høyesteretts praksis, jf. Rt. 2012 side 1556 med

videre henvisninger.

Datatilsynet legger derfor til grunn at det kreves klar sannsynlighetsovervekt for lovovertredelse for å kunne ilegge gebyr. Saksforholdet og spørsmålet om å ilegge overtredelsesgebyr er vurdert med utgangspunkt i dette beviskravet.

Det vises i denne sammenheng til kapittel IX i forvaltningsloven om «Administrative sanksjoner». Med en administrativ sanksjon menes en negativ reaksjon som kan ilegges av et forvaltningsorgan, som retter seg mot en begått overtredelse av lov, forskrift eller individuell avgjørelse, og som regnes som straff etter den europeiske menneskerettskonvensjonen (EMK).

For foretak er skyldvurderingen særegen. I forvaltningsloven § 46 (1) heter det:

> *«Når det er fastsatt i lov at det kan ilegges administrativ sanksjon overfor et foretak, kan sanksjonen ilegges selv om ingen enkeltperson har utvist skyld».*

I Prop. 62 L (2015-2016) side 199 uttales det om § 46: «Formuleringen om at 'ingen enkeltperson har utvist skyld' er hentet fra paragrafen om foretaksstraff i straffeloven § 27 første ledd og skal forstås på samme måte. Ansvaret er derfor som utgangspunkt objektivt».

Som nevnt over gir artikkel 83 i utgangspunktet anvisning på at ileggelse av overtredelsesgebyr beror på en skjønnsmessig helhetsvurdering, men legger føringer på skjønnsutøvelsen ved å trekke frem momenter som skal ha særlig vekt, idet det ses hen til at ileggelse av overtredelsesgebyr i hvert enkelt tilfelle skal være virkningsfull, forholdsmessig og avskrekkende.

Vi har særlig lagt vekt på følgende momenter i vår vurdering:

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

SVV og bompengeselskapene har innført ny systemløsning for innkreving av avgifter ved passeringer i bompengeringen. Det nye systemet skal iht. SVV fungere slik at passeringshistorikk skal kunne slettes på en måte som ligger innenfor personvernforordningens krav. Problemet knytter seg til den gamle systemløsningen som ikke hadde en slik funksjonalitet. Passeringsdata slettes ikke i denne systemløsningen. Dette går langt tilbake i tid. Klager har i dokumentasjon (vedlegg 1) påvist at det i systemet er registrert opplysninger tilbake til 2011.

I personvernerklæringen til Fjellinjen opplyses det at for kjøretøy med avtale registreres personopplysninger i tråd med avtalevilkårene, mens kjøretøy uten avtale registreres med videobilde av bilens registreringsnummer. I tillegg viste det seg at det var registrert bostedsadresse i systemet fra 2008 og 2010. Det indikerer at det i systemet er registrert

personopplysninger som det ikke er lovlig å behandle, jf. artikkel 5 nr.1 a) og artikkel 6 og artikkel 17 nr. 1 a) og d).

Det er, slik Datatilsynet ser det, ikke lov, og derfor ikke behandlingsgrunnlag etter artikkel 6, til å behandle passeringsdata utover bokføringsforskriftens krav. Omfanget er betydelig, og har vært virkende over lang tid. Passeringsdata regnes ikke som en særlig kategori av personopplysninger, jf. artikkel 9, men oppleves for mange som beskyttelsesverdig, ettersom slike opplysninger vil kunne si noe om den enkeltes bevegelsesmønster. Hvis man bruker bilen daglig vil bevegelsesmønsteret nærmest bli komplett.

Det er urovekkende at bompengesystemet har eksistert i nær 20 år uten at man har oppdaget den manglende slette-funksjonaliteten. Det tyder på manglende fokus på rettighetene til de registrerte og manglende testing av systemet.

På EDBs (European Data Protection Board) hjemmeside 5. november 2019 omtales et vedtak fra det tyske datatilsynet, som ga eiendomsselskapet Deutsche Wohnen et gebyr på 14, 5 millioner euro for overtredelse av bestemmelser i personvernforordningen. Under et tilsyn i juni 2017 og mars 2019 fant tilsynsmyndigheten at selskapet brukte et arkivsystem for lagring av personopplysninger om leietakere som ikke gjorde det mulig å slette personopplysninger som ikke lenger var nødvendig.

*b) **hvorvidt overtredelsen ble begått forsettlig eller uaktsomt***

SVV har hatt kunnskap om denne funksjonalitetsbristen i lengre tid, og har slik Datatilsynet ser det ikke gjort tilstrekkelige tiltak for å endre på dette. Funksjonsfeilen har eksistert i systemløsningen fra starten av. Dette har således også vært et brudd på bestemmelsene i den gamle personopplysningsloven (2000). Kravet til at registrering av passeringsdata skulle ha behandlingsgrunnlag fulgte også av gammel personopplysningslov § 8.

SVV har hatt en løpende dialog med Datatilsynet fra i april 2019 om å få på plass en funksjonalitet i det gamle systemet slik at passeringsdata ble slettet. Dette arbeidet har tatt tid, og som det går fram av vedlagte dokumentasjon har partene tydelig ikke vært enig om hvem som hadde ansvar for at dette dro ut i tid. Datatilsynet ønsker å bemerke at dette ikke har vesentlig betydning da denne funksjonalitet skulle vært på plass fra starten av. Og dette ansvar påligger SVV.

Vi vurderer det som hevet over tvil at SVV har hatt kunnskap om nødvendigheten for etablering av organisatoriske og tekniske tiltak i systemet. Ved ikke å ta de nødvendige skrittene, har SVV handlet grovt uaktsomt.

Datatilsynet finner at det er en klar sannsynlighetsovervekt for at SVV har overtrådt artiklene 5, 17 og 25 i personvernforordningen.

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

SVV arbeider sammen med Q-Free for å få på plass en funksjonalitet i den gamle systemløsningen som innebærer at sletting kan skje.

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***

Personvernforordningen har innført en langt høyere grad av ansvarlighet for den behandlingsansvarlige, jf. ansvarlighetsprinsippet i artikkel 5 nr. 2. SVV har ikke sikret at den gamle systemløsningen hadde nødvendig funksjonalitet. Det kan derfor konstateres at SVV har handlet kritikkverdig i forhold til å sikre at løsningen var i samsvar med personvernforordningen.

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

Ingen tidligere overtredelser kan konstateres.

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

Fra våren 2019 har Datatilsynet vært informert om arbeidet med å få en ny funksjonalitet på plass i den gamle løsningen.

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

Personopplysninger som har vært registret er passeringsdata i bomringen. I tillegg har nødvendige opplysninger for å kunne utstede faktura vært registrert.

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

Datatilsynet fikk kunnskap om dette gjennom det krav klager framsatte overfor Fjellinjen høsten 2018.

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 har ikke tidligere vært gjennomført tiltak overfor SVV med hensyn til samme saksgjenstand.

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

Ikke relevant for saken.

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

Datatilsynet har ikke konstatert at SVV har hatt økonomiske fordeler, eller unngått tap direkte eller indirekte som et resultat av overtredelsen. Det kan heller ikke anføres noe i formildende retning.

Datatilsynet har heller ikke tatt hensyn til SVVs økonomiske evne.

6.4 Oppsummering

I vurderingen av om overtredelsesgebyr skal ilegges, legger Datatilsynet særlig vekt på at overtredelsene betydelig har krenket grunnleggende prinsipper som forordningen verner, jf. forordningen artikkel 5 nr. 1, artikkel 6, artikkel 17 og artikkel 25.

Datatilsynet legger særlig vekt på at SVV i lengre tid har behandlet personopplysninger uten behandlingsgrunnlag. Datatilsynet vurderer dette som alvorlig. Borgerne har en klar og beskyttelsesverdig interesse mot at det behandles personopplysninger uten at dette er lov. Allmennpreventive grunner og hensynet til at reglene skal ha effekt og virke etter sin hensikt, taler da med styrke for at det reageres med et virkemiddel som overtredelsesgebyr.

Datatilsynet kan ikke se at de øvrige momenter som loven fremhever gjør seg gjeldende i nevneverdig grad – verken i skjerpende eller formildende retning.

Konklusjon

Datatilsynet er etter dette kommet til at overtredelsesgebyr bør ilegges.

6.5 Gebyrets størrelse

Når det gjelder gebyrets størrelse, skal de samme momenter som ved vurdering av om gebyr skal ilegges, tillegges særlig vekt. De forhold Datatilsynet har pekt på ovenfor taler for et gebyr av en viss størrelse. Gebyret bør settes så høyt at det får virkning også utover den konkrete saken. Samtidig må gebyrets størrelse stå i et rimelig forhold til overtredelsen og virksomheten.

Vi har særlig sett hen til at SVV i den gamle systemløsningen ikke har etablert en funksjonalitet som gjorde at personvernforordningen kunne etterleves. Videre har vi sett på den generelle forventning borgerne skal kunne ha til at statlige instanser følger de regler som er gitt, og særlig de som gir enkeltindivider rettigheter som er ment å være en beskyttelse for disse.

I en lignende sak utstedte Berlin Commissioner for Data Protection (tyske datatilsynet) 30. oktober 2019 en bot på 14,5 millioner euro mot Deutsche Wohnen SE for brudd på GDPR. Eiendomsselskapet hadde et arkivsystem for lagring av personopplysninger om leietakere hvor det ikke var mulig å slette personopplysninger som ikke lenger var nødvendige. Personopplysningene ble lagret uten at selskapet kontrollerte hvorvidt personopplysningene var nødvendige. Gjennom tilsyn i 2017 og 2019 kunne det tyske datatilsynet konstatere at personopplysninger som ikke lenger var nødvendige ikke lot seg slette. I en pressemelding av 5. november 2019 fra Berlin Commissioner for Data Protection heter det at selv om selskapet var med på å avhjelpe manglene var det nødvendig å utstede et overtredelsesgebyr for brudd på personvernforordningen artikkel 25 og artikkel 5.

Det tyske datatilsynet slo fast at lagringen var et brudd på grunnprinsippene i personvernforordningen (artikkel 5) og innebygd person (artikkel 25). At systemet var anskaffet før personvernforordningen trådte i kraft hadde således ingen betydning.

Saken med Deutsche Wohnen har klare paralleller til denne saken:

- personopplysninger i arkivsystemet lot seg ikke slette
- selskapet hadde vært behjelpelig med å avhjelpe manglene
- personopplysningene kunne ikke beviselig sies å være misbrukt
- arkivsystemene var etablert før personvernforordningen trådte i kraft
- selskapet kontrollerte ikke hvorvidt personopplysningene lot seg slette
- ingen har hatt innebygd personvern eller personvern som standardinnstilling

Signalvirkningen av denne saken, de allmennpreventive hensyn, mener vi er tydelige. Det bør være en vekker for SVV for hvordan man forvalter personopplysning om de som passerer i bomringen.

Etter en totalvurdering av saken og da særlig sett hen til alvorligheten i overtredelsen har vi kommet til at et overtredelsesgebyr på **4.000.000** anses riktig.

Tilsvar
Vedtaket blir fattet med mindre Datatilsynet, innen **mandag 23. mars 2020**, har mottatt redegjørelse som tilsier at situasjonen ikke er i samsvar med det vi har beskrevet over. Datatilsynet forutsetter at kommunen umiddelbart iverksetter skadereduserende tiltak.

Med vennlig hilsen

Bjørn Erik Thon
direktør

Knut Brede Kaspersen
juridisk fagdirektør

Vedlegg: Sakens dokumenter

Kopi til: Ole Østlid, Cappelens gate 40, 3015 DRAMMEN