Datatilsynet

EAS / ELEKTRO & AUTOMASJON SYSTEMER AS
Åshaugveien 62

3170 SEM

Unntatt offentlighet:
Offl. § 13 jf. Popplyl. § 24 (1) 2. pkt.

Deres referanse	Vår referanse	Dato
	20/04401-11	13.12.2021

Vedtak om pålegg og overtredelsesgebyr - Klage på kredittvurdering uten saklig behov - EAS /Elektro & Automasjon Systemer AS

1. Innledning

Vi viser til vårt varsel om vedtak om pålegg og overtredelsesgebyr datert 17. juni 2021. Vi viser også til deres merknader til varselet datert 15. juli 2021. Disse merknadene behandles i vedtakets punkt 7.1 og 8.3.

2. Vedtak om pålegg og overtredelsesgebyr

1. *Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i ilegges EAS /* Elektro & *Automasjon Systemer AS, org.nr. 991 800 492, et overtredelsesgebyr til statskassen på 200 000 kroner for å ha innhentet kredittopplysninger uten rettslig grunnlag, jf. personvernforordningen artikkel 6 nr. 1 bokstav f.*

2. *Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav d pålegges EAS / Elektro* & Automasjon *Systemer AS å utbedre internkontroll og rutiner for kredittvurderinger, jf. personvernforordningen artikkel 24.*

3. Nærmere om sakens faktiske forhold

Vi mottok 18. november 2020 en klage fra [redacted] (heretter «klager»), om at EAS / Elektro & Automasjon Systemer AS hadde gjennomført en kredittvurdering av han. Klager fikk informasjon 6. oktober 2020 om at det hadde blitt gjennomført en kredittvurdering.

Klager opplyser om at vedkommende ikke har hatt noe samarbeid, kundeforhold eller annen tilknytning til deres virksomhet. Han hadde ingen forventning om at han skulle bli

kredittvurdert av virksomheten og opplever hendelsen som unødvendig «grafsing» i hans privatøkonomi.

I deres svar på vårt krav om redegjørelse bekrefter dere at klager hverken er kunde hos dere eller har annen direkte relasjon til EAS / Elektro & Automasjon Systemer AS. Dere beskriver at dere bruker Bisnode som verktøy for å gjøre kredittsjekk av bedrifter som er kunder, leverandører og firma i samme bransje. Kredittsjekken av klager skal ha skjedd ved en feiltakelse som følge av manglende kunnskap om systemet i Bisnode.

Dere beskriver videre at dere årlig går igjennom regnskap til andre aktører i bransjen for å vurdere egen prestasjon. Klager er del-eier av firmaet [redacted] som er i samme bransje som EAS / Elektro & Automasjon Systemer AS. I prosessen med å se på regnskapet til [redacted], ble det klikket på klagers navn i oversikten over aksjonærer. Dere forklarer at daglig leder forventet at han da ville få opp en oversikt over eierinteresser, tilsvarende det som er systemet på proff.no og purehelp.no.

Dere viser til at hverken virksomheten eller daglig leder privat har interesse av å innhente kredittopplysninger om klager. Informasjon innhentet i Bisnode ble ikke skrevet ut eller lagret på noen måte i virksomheten, og det ble antatt at søket ble avbrutt. Dere viser også til at det er første gang en slik kredittsjekk av en privatperson er utført av EAS / Elektro & Automasjon Systemer AS.

I redegjørelsen skriver dere at dere har vært i kontakt med Bisnode for å få kredittvurderingsverktøyet forklart i etterkant av at dere mottok Datatilsynets krav om redegjørelse. Dere viser til at dere har rutiner for behandling av personopplysninger i virksomheten, men at disse rutinene ikke nevner kredittvurdering. Videre skriver dere at denne saken skal avviksbehandles hos dere og at rutiner skal gjennomgås for eventuelle endringer eller presiseringer.

Datatilsynet sendte et varsel om vedtak om pålegg og overtredelsesgebyr 17. juni 2021. EAS / Elektro & Automasjon Systemer AS innga merknader til dette varselet 20. juli 2021. Merknadene er behandlet under punktene 7.1 og 8.3 i dette vedtaket.

4. Behandlingsansvar

Den som bestemmer formål og midler for en behandling av personopplysninger, er behandlingsansvarlig, jf. personvernforordningen artikkel 4 nr. 7. Den behandlingsansvarlige er ansvarlig for at behandlingen av personopplysninger skjer i tråd med de grunnleggende prinsippene i personvernforordningen og skal kunne påvise dette, jf. personvernforordningen artikkel 5 nr. 2.

En virksomhet er ansvarlig for en behandling av personopplysninger utført av en ansatt når behandlingen har skjedd gjennom virksomhetens aktiviteter.[1] Det er EAS / Elektro &

[1] Det europeiske personvernrådets retningslinjer, EDPB Guidelines 07/2020 on the concept of controller and processor in the GDPR, s. 10.

Automasjon Systemer AS som har avtale med Bisnode og som etter vår vurdering har bestemt formålet og midlene med kredittvurderingene.

Den behandlingsansvarlige har plikt til å gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen skjer i samsvar med personvernforordningen, jf. artikkel 24.

Ifølge artikkel 24, skal man ved vurderingen av egnede tiltak ta hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for de registrertes rettigheter og friheter. Tiltakene skal gjennomgås på nytt og oppdateres ved behov.

Basert på dette anser Datatilsynet EAS / Elektro & Automasjon Systemer AS som behandlingsansvarlig etter personvernforordningen artikkel 4 nr. 7 for den aktuelle kredittsjekken som ble gjort av klager.

5. Rettslig grunnlag for innhenting av kredittopplysninger

5.1. Særlig om rettslig grunnlag for innhenting av kredittopplysninger

Å innhente og lagre kredittopplysninger om enkeltpersoner og enkeltpersonforetak utgjør en behandling av personopplysninger, jf. personvernforordningen artikkel 4 nr. 2 og lov om behandling av personopplysninger av 15. juni 2018 nr. 38 (personopplysningsloven) § 1.

Personvernforordningen artikkel 6 nr. 1 krever at all behandling av personopplysninger har et rettslig grunnlag. Når en virksomhet skal innhente kredittopplysninger om den registrerte uten at det foreligger samtykke, eller kredittvurderingen er strengt nødvendig for å gjennomføre en avtale med den registrerte, er artikkel 6 nr. 1 bokstav f det mest aktuelle rettsgrunnlaget.

Etter den gamle personopplysningsloven av 2000 gjaldt et tilleggskrav om at virksomheten måtte ha «saklig behov» for å innhente kredittopplysninger. Dette fremgår av personopplysningsforskriften § 4-3, som etter overgangsreglene[2] er videreført som gjeldende rett.

Den nye kredittopplysningsloven[3] viderefører også kravet om «saklig behov» for utlevering av kredittopplysninger. Den nye loven er vedtatt, men er ikke trådt i kraft ennå. Personvernforordningen gir imidlertid ikke nasjonalt handlingsrom for å særregulere den enkelte mottakers behandling av kredittopplysninger. Den nye kredittopplysningsloven har derfor kun kredittopplysningsvirksomhetene som pliktsubjekt, og ikke den enkelte virksomheten som bestiller kredittopplysninger.

Konsekvensen av dette er at «saklig behov» ikke direkte er et tilleggsvilkår for den enkelte virksomheten som innhenter kredittopplysninger. Deres innhenting reguleres altså av

[2] Overgangsregler om behandling av personopplysninger (FOR-2018-06-15-877).
[3] Lov om behandling av opplysninger i kredittopplysningsvirksomhet (LOV-2019-12-20-109).

personvernforordningen artikkel 6 nr.1 bokstav f. Vurderinger knyttet til om en virksomhet har «saklig behov» etter personopplysningsforskriften § 4-3 har imidlertid nær sammenheng med vurderingen etter artikkel 6 nr. 1 bokstav f. Tidligere praksis knyttet til «saklig behov» er derfor fortsatt relevant ved vurdering av «berettiget interesse» som behandlingsgrunnlag.

5.2. Personvernforordningen artikkel 6 nr. 1 bokstav f – «berettiget interesse»

Artikkel 6 nr. 1 bokstav f krever at innhenting av kredittopplysninger er «nødvendig» for å ivareta en «berettiget interesse» som etter en interesseavveining veier tyngre enn hensynet til den enkeltes personvern.

Den berettigede interessen må være lovlig, klart definert på forhånd, reell og saklig begrunnet i virksomheten. Fortalepunkt 47 til personvernforordningen angir at det i vurderingen av om en interesse er berettiget, blant annet skal tas hensyn til den registrertes forventinger basert på forholdet mellom den behandlingsansvarlige og den registrerte. Det skal også legges vekt på om det på innsamlingstidspunktet var påregnelig for de registrerte at opplysningene ville bli behandlet for det aktuelle formålet.

Hvilke interesser som oppfyller dette beror på en helhetlig vurdering av blant annet hvilke fordeler virksomheten oppnår med behandlingen, hvor viktig interessen er for virksomheten, om behandlingen har offentlig interesse eller ivaretar den ideelle interesser som kommer flere til gode, se Artikkel 29-gruppens uttalelse.[4]

Videre må den aktuelle behandlingen av personopplysninger være nødvendig for denne interessen. Det vil si at virksomheten må vurdere om den kan oppnå formålet på en måte som bedre ivaretar personvernet. Man må altså velge den behandlingen som er minst inngripende.

Deretter må virksomheten foreta en interesseavveining for å avgjøre om den enkeltes personvern veier tyngre enn virksomhetens berettigede interesse. Hvilke type opplysninger det er snakk om er relevante momenter for interesseavveiningene, f.eks.om disse er beskyttelsesverdige og om personen har en forventning om å få ha personopplysningene i fred. Det er også relevant å vurdere hva slags ulemper behandling av personopplysningene påfører personen, hvorvidt behandlingen av personopplysningene oppleves som krenkende, om behandlingen er egnet til å skape frykt eller uro, og hvilke tiltak virksomheten har iverksatt for å redusere personvernkonsekvensene.

5.3. Relevant praksis knyttet til personopplysningsforskriften § 4-3 – «saklig behov»

Ifølge personopplysningsforskriften § 4-3 kan kredittvurdering kun innhentes når en virksomhet har et «saklig behov» for opplysningene, for eksempel i forbindelse med et kjøp på kreditt. Det må altså som hovedregel foreligge et kredittelement. Dette vil typisk være når virksomheten skal yte kreditt til en kunde og trenger å se om vedkommende er kredittverdig.

[4] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, side 24 og 25.

Personvernnemnda har utdypet tilleggsvilkåret om saklig behov i flere saker, blant annet PVN-2006-03 KLP, PVN-2010-05 Kredittvurdering og PVN-2017-02 Bertram Bil. I sistnevnte sak henviste nemnda til følgende uttalelse fra PVN-2006-03 KLP:

> Formålet med en kredittvurdering er normalt å kartlegge hvorvidt en potensiell kunde er kredittverdig, og dermed om selskapet ønsker å inngå avtale med vedkommende. Det vil si at når det bes om kredittopplysninger vil saklighetskravet være oppfylt når bestilleren skal benytte kredittopplysningene i forbindelse med sin vurdering av kredittrisiko, for eksempel ved et tilsagn om lån eller avtale om løpende ytelser som faktureres etterskuddsvis, typisk mobiltelefonabonnement, abonnement på satellittfjernsyn etc.

Nemnda henviste også til uttalelse i PVN-2010-05 Kredittvurdering, hvor det ble uttalt at det motsatte av «saklig behov» er «nysgjerrighet og kikkermentalitet».

6. Om plikten til å gjennomføre egnede tekniske og organisatoriske tiltak

Etter personvernforordningen artikkel 24 skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med personopplysningsloven og personvernforordningen.

Dersom det står i et rimelig forhold til behandlingsaktivitetene, skal virksomheten iverksette egnede retningslinjer for vern av personopplysninger.

Kredittvurdering er en inngripende behandling av personopplysninger og utgjør et stort inngrep i enkeltpersoners rett til personvern. Virksomheter som gjennomfører kredittvurderinger må derfor dokumentere sine interne rutiner eller prosesser (internkontroll), som ivaretar kravet om saklighet ved kredittvurdering. Rutinene skal beskrive når og hvordan kredittopplysninger kan innhentes og hvordan innsyn skal gis. Rutinene skal sikre at kredittopplysninger ikke innhentes uten at kravet om saklig behov er oppfylt.

7. Datatilsynets vurdering

7.1. Plikten til internkontroll og ansvarlighetsprinsippet

Det kommer fram av redegjørelsen at EAS / Elektro & Automasjon Systemer AS hadde rutiner for behandling av personopplysninger, men at disse ikke inkluderte rutiner for gjennomføring av kredittvurderinger. Vi legger til grunn at EAS / Elektro & Automasjon Systemer AS ikke hadde rutiner for kredittvurderinger på kontrolltidspunktet.

I redegjørelsen forklarer dere at daglig leders manglende forståelse for kredittvurderingsverktøyet var årsak til at den aktuelle kredittvurderingen ble gjennomført. Dere viser til at dere bruker Bisnode til kredittsjekk av bedrifter som er kunder, leverandører og firmaer i samme bransje. Selv om dere normalt ikke vil innhente kredittopplysninger om privatpersoner, tilsier tilgangen til kredittvurderingsverktøyet at dere må ha en bevissthet rundt regelverket og funksjonene i Bisnode når det kommer til innhenting av kredittopplysninger om fysiske personer og enkeltmannsforetak.

Den manglende bevisstheten om regelverket, virksomhetens tilgang til kredittvurderingstjenester, samt at det har skjedd et brudd på regelverket i denne saken tilsier at EAS / Elektro & Automasjon Systemer AS pålegges å etablere internkontroll for kredittvurderinger. Etter vår vurdering vil etablering av rutiner kunne virke preventivt mot at det senere blir gjennomført urettmessige kredittvurderinger.

I sine merknader til Datatilsynets varsel, har EAS / Elektro & Automasjon Systemer AS lagt ved reviderte rutiner for behandling av personopplysninger med en ny «Rutine 8: Rutine for kredittvurdering, jf. personvernforordningen artikkel 24». I rutinen er det inkludert en gjengivelse av personvernforordningen artikkel 24 og en kort beskrivelse av hvem som kan gjennomføre kredittvurdering og i hvilke tilfeller kredittvurdering kan gjennomføres.

Datatilsynet mener at det er positivt at det er gjort en klar avgrensning av hvem som kan gjennomføre kredittvurderinger. Likevel, rutinene bør vise til hvilket rettslig grunnlag virksomheten har for kredittvurderinger i tilfelle privatpersoner og enkeltmannsforetak blir kredittvurdert. Rutinen bør i større grad knyttes opp til reglene og vurderingene som skal gjøres etter personvernregelverket. Det er viktig å være oppmerksom på at personvernreglene gjelder for kredittvurdering av enkeltmannsforetak, da denne informasjonen er tett knyttet til informasjon om økonomien til privatpersonen som har foretaket.

EAS / Elektro & Automasjon systemer AS bør i sine rutiner fremheve artikkel 6 nr. 1 bokstav f som relevant behandlingsgrunnlag for deres virksomhet, samt sørge for organisatoriske tiltak som sikrer at kravene i personvernforordningen er oppfylt før kredittopplysninger om privatpersoner og enkeltpersonforetak innhentes.

Datatilsynet har kompetanse til å pålegge den behandlingsansvarlige å sørge for at behandlingsaktivitetene skjer i samsvar med bestemmelsene i personvernforordningen, jf. personvernforordningen artikkel 58 nr. 2 bokstav d. Dette er bakgrunnen for pålegget om å utbedre rutiner for kredittvurdering.

EAS / Elektro & Automasjon Systemer AS må utbedre rutinene for å sikre at kredittvurdering bare skjer når vilkårene i personvernforordningen er oppfylt.

7.2. Behandlingsgrunnlag for innhenting av kredittopplysninger
Spørsmålet er om EAS / Elektro & Automasjon Systemer AS hadde et gyldig behandlingsgrunnlag etter artikkel 6 nr. 1 bokstav f da dere innhentet kredittopplyser om klager.

Det første vilkåret som må være oppfylt for at behandlingen skal være lovlig er at EAS / Elektro & Automasjon Systemer AS hadde en «berettiget interesse» i å innhente opplysningene.

EAS / Elektro & Automasjon Systemer AS skriver i deres redegjørelse at det er riktig slik klager påpeker at han hverken er kunde eller har andre direkte relasjoner til virksomheten. Videre skriver dere at dette ble gjort ved en feil idet man ønsket å få opplysninger om

eierinteresser i et selskap hvor klager er del-eier. Uavhengig av om det ble gjort med overlegg eller ikke, så har EAS / Elektro & Automasjon Systemer AS innhentet kredittopplysninger om en enkeltperson uten noen form for kundeforhold, leverandørforhold eller annen tilknytning til virksomheten. Det er enighet mellom partene om at kredittvurderingen ikke skulle vært utført. Klager hadde ingen forventning om at EAS / Elektro & Automasjon Systemer AS skulle behandle hans kredittopplysninger og det var heller ikke påregnelig at virksomheten skulle innhente opplysningene.

Vår vurdering er at kravet til «berettiget interesse» i personvernforordningen artikkel 6 nr. 1 bokstav f ikke er oppfylt.

Vi anser det ikke hensiktsmessig å vurdere kravet om «nødvendighet» ettersom vår vurdering er at virksomheten ikke hadde en berettiget interesse til å gjennomføre kredittvurderingen.

Det tredje vilkåret i artikkel 6 nr. 1 bokstav f er den konkrete interesseavveiningen mellom virksomhetens interesse i å behandle personopplysningene og de registrertes personverninteresser.

Kredittopplysninger er en type personopplysninger som er særlige beskyttelsesverdige. En kredittvurdering er et resultat av sammenstilling av personopplysninger fra mange ulike kilder, og viser et tall som angir sannsynligheten for at en person vil betale en fordring. En kredittvurdering vil også vise detaljer om enkeltpersoners privatøkonomi, herunder eventuelle betalingsanmerkninger, frivillige pantstillelser og gjeldsgrad. Dette er private opplysninger som privatpersoner har en forventning om at ikke innhentes av virksomheter med mindre det er saklig begrunnet i deres forhold til dem. Privatpersoner bør derfor nyte et særlig vern mot innhenting av kredittopplysninger.

Hensynet til klagernes rett til personvern veier tungt ved behandling av denne typen personopplysninger. Virksomheten hadde ikke behov for å innhente kredittopplysninger om klager og en eventuell innhenting av kredittopplysninger på bakgrunn av nysgjerrighet vil ikke oppfylle interesseavveiningen i artikkel 6 nr. 1 bokstav f.

Konklusjonen er etter dette at EAS / Elektro & Automasjon Systemer AS ikke hadde rettslig grunnlag etter artikkel 6 nr. 1 bokstav f for å behandle kredittopplysninger om klager meddelt klager 6. oktober 2020.

8. Overtredelsesgebyr

8.1. Generelt om overtredelsesgebyr

Overtredelsesgebyr er et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsregelverket. Vi mener det er nødvendig å reagere på overtredelsen, og varsler med dette ileggelse av 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.

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).

8.2. Vurdering av om overtredelsesgebyr skal ilegges

Ved vurderingen av om det skal ilegges gebyr og ved utmålingen skal Datatilsynet ta hensyn til momentene i personvernforordningen artikkel 83 nr. 2 bokstav a) til k). Datatilsynet kan ilegge overtredelsesgebyr etter en skjønnsmessig helhetsvurdering, men de opplistede momentene legger føringer på skjønnsutøvelsen ved å trekke frem momenter som skal tillegges særlig vekt.

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,

Lovlighetsprinsippet i personvernforordningen artikkel 5 nr. 1 og kravet til behandlingsgrunnlag i artikkel 6 er et av de grunnleggende kravene som skal oppfylles når en virksomhet behandler personopplysninger.

Som vi har redegjort for over er kredittopplysninger en type personopplysninger som er særlige beskyttelsesverdige og som privatpersoner har en forventning om at ikke innhentes av virksomheter, med mindre det er saklig begrunnet i deres forhold til dem. Klager har ikke hatt noe forhold til virksomheten som gjorde det påregnelig at dere skulle behandle kredittopplysninger om han. Overtredelsen er derfor alvorlig, og tilsier at det ilegges overtredelsesgebyr.

I formildende retning trekker det faktum at en ulovlig kredittvurdering ikke vil være en overtredelse over lengre varighet. I denne saken viser EAS / Elektro & Automasjon Systemer AS til at dere trodde søket ble avbrutt og at dere ikke har lagret kredittopplysninger om klager i virksomheten. Skaden er imidlertid skjedd i det øyeblikket personlige kredittopplysninger blir innhentet og behandlet av noen uten behandlingsgrunnlag.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt,

Dere beskriver at kredittvurderingen skal ha blitt utført ved et uhell, da daglig leder forventet å få informasjon om eierinteresser i selskapet klager er del-eier i da han trykket på klagers

navn i oversikten over aksjonærer. Videre kommer det fram av redegjørelsen at hverken daglig leder personlig eller EAS / Elektro & Automasjon Systemer AS hadde interesse av å få tilgang til klagers kredittopplysninger. Det foreligger ikke holdepunkter for å konkludere med at kredittvurderingen ble gjort forsettlig.

Det må imidlertid kunne forutsettes at daglig leder i et firma har kjennskap til sentrale funksjoner ved kredittvurderingsverktøyet bedriften benytter seg av. Datatilsynet legger til grunn at virksomheten, ved daglig leder, har utvist uaktsomhet ved innhentingen av kredittopplysninger om klager.

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

I redegjørelsen vises det til at daglig leder antok at søket ble avbrutt og at det ikke ble lagret kredittopplysninger om klager i virksomheten. Dette trekker derfor ikke i skjerpende retning.

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,

Vi legger i skjerpende retning vekt på at overtredelsene ble utført av daglig leder i virksomheten, ettersom personvernforordningen forutsetter at etterlevelse av regelverket er særlig forankret hos ledelsen i en virksomhet, jf. artikkel 5 nr. 2.

Videre legger vi vekt på i skjerpende retning at EAS / Elektro & Automasjon Systemer AS hadde manglende bevissthet om regelverket, samt at virksomheten hverken hadde tekniske eller organisatoriske tiltak i form av rutiner for å sikre etterlevelse av regelverket og den nødvendige kunnskapen om kredittvurderingsverktøyet virksomheten benytter seg av.

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

Datatilsynet kjenner ikke til om det foreligger tidligere overtredelser.

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

Virksomheten beklager hendelsen og har vist vilje til å bidra til sakens opplysning og til å lære av hendelsen ved å behandle saken i deres avvikssystem, gå igjennom og justere rutiner for behandling av personopplysninger i virksomheten. Dette trekker derfor ikke i skjerpende retning.

g) kategoriene av personopplysninger som er berørt av overtredelsen,

Særlige kategorier av personopplysninger (sensitive personopplysninger) er ikke berørt av overtredelsen i vår sak. Opplysninger om lønn, gjeld og kredittverdighet er imidlertid opplysninger som har et særlig beskyttelsesbehov på grunn av deres private karakter. Dette trekker i skjerpende retning.

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

Vi ble underrettet om overtredelsen av klager. Virksomheten underrettet ikke selv om overtredelsen. Dette kan i noen tilfeller trekke i skjerpende retning, men Datatilsynet har ikke vektlagt dette i særlig skjerpende retning i denne saken da det ikke foreligger konkrete holdepunkter for at EAS / Elektro & Automasjon Systemer AS skulle opptrådt annerledes overfor Datatilsynet i dette tilfellet.

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,

Vi kjenner ikke til at det tidligere er truffet tiltak overfor virksomheten med hensyn til samme saksgjenstand. Dette trekker derfor ikke i skjerpende retning.

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

Vi finner ikke dette momentet relevant.

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 kan ikke se at EAS / Elektro & Automasjon Systemer AS har oppnådd noen fordeler som følge av overtredelsen, og vi vektlegger ikke dette momentet i skjerpende retning.

Basert på vurderingen ovenfor kommer Datatilsynet til at overtredelsesgebyr bør ilegges. Det neste spørsmålet er gebyrets størrelse.

8.3. Vurdering av gebyrets størrelse

Ved utmåling av gebyrets størrelse skal det legges vekt på de samme vurderingsmomentene som i spørsmålet om hvorvidt gebyr bør ilegges. Vi viser derfor til vurderingene av sakens alvorlighet ovenfor. Overtredelsesgebyret skal 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.

Gebyret bør settes så høyt at det får virkning også utover den konkrete saken, samtidig som gebyrets størrelse må stå i et rimelig forhold til overtredelsen og virksomheten, jf. artikkel 83 nr. 1.

Personvernforordningen legger til rette for et høyere bøtenivå enn det som gjaldt etter personopplysningsloven fra 2000, og det følger av forordningens artikkel 83 nr. 1 at overtredelsesgebyr skal fastsettes konkret slik at det i hvert enkelt tilfelle er virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende. Hovedformålet med overtredelsesgebyr er prevensjon, altså at risikoen for å bli ilagt gebyr skal virke avskrekkende og derved medvirke til økt etterlevelse av regelverket.[5]

Av Skullerud m.fl. (2019), side 347, fremgår det:

> Prevensjonshensynet tilsier at gebyret for en overtredelse må settes så høyt at denne faktisk oppleves som et onde av overtrederen. Dette innebærer at overtrederens økonomiske evne bør ha betydning ved utmålingen, slik at gebyret blir høyere desto sterkere bæreevne overtrederen har. […] Ved vurdering av økonomisk bæreevne for et foretak kan det være relevant å se hen til foretakets samlede globale årsomsetning i forutgående regnskapsår, jf. art. 83 nr. 4 og 5.

Og videre:

> Hensynet til å sikre en individuell vurdering i hvert enkelt tilfelle tilsier at tilsynsmyndighetene bør unngå å etablere standardiserte gebyrsatser. Dette gjelder selv om nasjonal rett åpner for standardiserte satser, jf. forvaltningsloven § 43.

Gebyret skal altså utmåles konkret i hvert tilfelle, og virke avskrekkende for den enkelte virksomheten.

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.

I vår sak manglet EAS / Elektro & Automasjon Systemer AS behandlingsgrunnlag for innhenting kredittopplysninger om klager (lovlighetsprinsippet). I tillegg manglet virksomheten tekniske og organisatoriske tiltak for etterlevelse av personvernregelverket (ansvarlighetsprinsippet). Manglende kunnskap om kredittvurderingsverktøyet og retningslinjer for når kredittvurdering kan gjennomføres, har lagt til rette for at kredittvurdering har blitt gjennomført ulovlig. Dette trekker i skjerpende retning.

I skjerpende retning legger vi særlig vekt på at kredittvurderingen ble igangsatt av virksomhetens daglige leder, og at virksomhetens ledelse manglet kunnskap om hvordan

[5] Skullerud et al. (2019).

kredittvurderingsverktøyet skulle brukes for å unngå å utføre ulovlige kredittvurderinger av privatpersoner.

Gebyret skal settes så høyt at det er virkningsfullt og oppnår tilstrekkelig avskrekkende effekt. I utmålingen av gebyrets størrelse legger vi derfor også vekt på virksomhetens økonomi. EAS / Elektro & Automasjon Systemer AS' merknader til størrelsen på det varslede gebyret har derfor betydning for utmålingen.

EAS / Elektro & Automasjon Systemer AS har kommet med flere merknader om virksomhetens økonomi knyttet til den pågående endrede situasjonen som følge av Covid-19-pandemien. EAS / Elektro og Automasjon Systemer AS opplyser om at virksomheten har gjennomført permitteringer det siste året for å tilpasse dere en situasjon med liten ordretilgang. På tidspunktet for merknadene er 7 ansatte i bedriften permittert, tilsvarende 24 % av arbeidsstokken. Dere viser til at i lys av dette, så bør gebyret reduseres vesentlig.

Det varslede gebyret på 250 000 kr er utmålt etter siste tilgjengelige regnskapstall fra 2019 på tidspunktet for varselet. I 2019 hadde EAS / Elektro & Automasjon Systemer AS registrerte driftsinntekter på 34 630 000 kr.

EAS / Elektro & Automasjon Systemer AS har oversendt regnskapstall for 2020 og foreløpige regnskapstall for periode 1-4 av 2021. I 2020 hadde virksomheten en omsetning på kr 33 095 228. Dette utgjør ca. 95 % av omsetningen for 2019. I periode 1-4 av 2021 hadde virksomheten driftsinntekter på kr 9 526 603. For samme periode i 2020 hadde virksomheten driftsinntekter på kr. 11 425 258. Driftsinntektene for periode 1-4 2021 utgjør ca. 83% av driftsinntektene for samme periode i 2020.

På bakgrunn av den økonomiske situasjonen virksomheten befinner seg i som følge av koronapandemien, er vår vurdering at et lavere gebyr vil kunne ha den preventive og avskrekkende effekten artikkel 83 forutsetter.

Etter å ha hensyntatt overtredelsenes alvorlighet og EAS / Elektro & Automasjon Systemer AS' merknader, setter Datatilsynet det endelige gebyret til kr 200 000. Vi har med dette redusert det varslede gebyret på 250 000 kr med ca. 20 %, tilsvarende EAS / Elektro & Automasjon Systemer AS' omsetningsfall mellom 2019 og periode 1-4 av 2021.

Vi minner om at brudd på personvernforordningen artikkel 6 kan medføre sanksjoner i form av overtredelsesgebyr på opptil 20 millioner euro, se personvernforordningen artikkel 83 nr. 5 bokstav a. Dette tilsvarer ca. 214 000 000 NOK. Gebyret som ilegges i denne saken, er således helt i det nederste sjiktet av hva forordningen foreskriver for slike regelverksbrudd.

9. Klagerett og videre saksgang

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.

Dersom dere ikke påklager pålegget om overtredelsesgebyr, er oppfyllelsesfristen 4 uker etter klagefristens utløp, jf. personopplysningsloven § 27.

Fristen for å gjennomføre pålegget pkt. 2 om skriftlige rutiner (internkontroll) er **4 uker** etter klagefristens utløp. Dersom dere ikke påklager pålegget pkt. 2, må dere innen denne fristen sende oss en skriftlig bekreftelse, samt dokumentasjon, på at pålegget om internkontroll er gjennomført.

10. 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.

Datatilsynet har taushetsplikt om hvem som har klaget til oss, og om klagerens personlige forhold. Taushetsplikten følger blant annet av personopplysningsloven § 24 og forvaltningsloven § 13. Som part i saken kan dere likevel bli gjort kjent med slike opplysninger av Datatilsynet, jf. forvaltningsloven § 13 b første ledd nr. 1. Dere har også rett til innsyn i sakens dokumenter, jf. forvaltningsloven § 18.

Vi gjør oppmerksom på at dere har taushetsplikt om opplysninger dere får av Datatilsynet om klagerens identitet, personlige forhold og andre identifiserende opplysninger, og at dere bare kan bruke disse opplysningene i den utstrekning det er nødvendig for å ivareta interessene deres i denne saken, jf. forvaltningsloven § 13 b andre ledd. Vi gjør også oppmerksom på at brudd på denne taushetsplikten kan straffes etter straffeloven § 209.

Hvis dere har spørsmål om saken, kan dere ta kontakt med Ida Småge Breidablikk på telefon 22 39 69 70.

Med vennlig hilsen

Jørgen Skorstad
avdelingsdirektør, jus

Ida Småge Breidablikk
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Kopi til: [redacted]