Datatilsynet

INNOVASJON NORGE
Postboks 448 Sentrum
0104 OSLO

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

Deres referanse	Vår referanse	Dato
	20/02042-21	18.05.2021

Vedtak om overtredelsesgebyr – Klage på kredittvurdering uten behandlingsgrunnlag - Innovasjon Norge

1. Innledning

Vi viser til vårt varsel om vedtak om overtredelsesgebyr 4. januar 2021 og merknadene deres til dette varselet av 25. januar 2021 («merknadene»).

2. Vedtak om overtredelsesgebyr

Datatilsynet vedtar følgende:

> *Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i pålegges Innovasjon Norge, org.nr. 986 399 445, å betale et overtredelsesgebyr til statskassen på kr 1 000 000 for å ha innhentet kredittvurderinger uten lovlig behandlingsgrunnlag, jf. personvernforordningen artikkel 6 nr. 1 bokstav f.*

3. Nærmere om sakens faktiske forhold

Vi mottok 17. april 2020 en klage fra («klager») om at Innovasjon Norge hadde gjennomført kredittvurderinger av 18. januar 2020 og 21. februar 2020. Etter at vi mottok klagen gjennomførte Innovasjon Norge en ny kredittvurdering av klager den 24. april 2020.

Klager opplyser at ikke har hatt noe samarbeid, kundeforhold eller annen tilknytning til Innovasjon Norge som kan begrunne kredittvurderingene. er derfor av den oppfatning at kredittvurderingene ikke har hatt et lovlig grunnlag.

Samlet sett har det blitt foretatt ti kredittvurderinger. Vi forstår at seks av disse er gjort av klagers selskap, mens til sammen fire kredittvurderinger er gjort av klager personlig og enkeltpersonforetak
Kredittvurderingene ble utført på følgende tidspunkt:

- 18. januar 2020
- 18. januar 2020
- 21. februar 2020
- 24. april 2020

Klagers selskap ble kredittvurdert på følgende tidspunkt:

- 18. januar 2020
- 19. januar 2020
- 21. januar 2020
- 24. februar 2020
- 26. februar 2020
- 6. mai 2020

Det er kun kredittvurderingene av klager personlig og enkeltpersonforetak som er gjenstand for vurdering etter personvernforordningen. Kredittvurderingene av klagers aksjeselskap er ikke omfattet av regelverket ettersom det ikke regnes som personopplysninger etter loven. Det er derfor kun kredittvurderingene av klager personlig og enkeltpersonforetak som sanksjoneres i dette vedtaket.

Kredittvurderingene ble ifølge dere foretatt med bakgrunn i en varslet søknad om finansiering fra en kunde. Dere skriver imidlertid i brev til oss 24. april 2020 at dere ikke hadde saklig grunn for å innhente kredittopplysninger om klager personlig, og at det ikke forelå behandlingsgrunnlag for behandlingen av personopplysninger. Likevel ble klagers enkeltpersonforetak kredittvurdert samme dag som brevet til oss er datert. Ifølge redegjørelsen fra dere skjedde denne kredittvurderingen på grunn av en misforståelse. En saksbehandler fikk videresendt en e-post som klager hadde sendt, og vedkommende trodde det dreide seg om en potensiell kunde. I merknadene skriver dere at innhenting av kredittopplysningene til klager har sin årsak i menneskelige feilvurderinger som har blitt fulgt opp i et arbeidsrettslig spor.

Av pressemeldingen 7. mai 2020 framgår det at brukeridentiteter og passord for tilgang til å gjøre kredittvurderinger er videreformidlet mellom kollegaer. Dette har skjedd ved at personlige brukeridentiteter og passord som gir tilgang til Bisnode er lånt ut. I redegjørelsen fra dere 10. august 2020 skriver dere at den ene kredittvurderingen av klagers enkeltpersonforetak ble foretatt av en medarbeider med slik videreformidlet tilgang.

Dere opplyser i e-posten 8. mai at tilgangene er suspendert og at dere vil foreta en fullstendig gjennomgang av retningslinjer og rutiner knyttet til kredittvurderinger. Rapporten fra PwC viser til en rekke anbefalinger som styret besluttet å følge opp i styremøtet 29. mai 2020.

Klager mener videre at det foreligger brudd på personopplysningssikkerheten fordi kredittsjekkene, etter vurdering, ble foretatt utenfor Innovasjon Norges lokaler, og dermed på et usikret nett. er også av den oppfatning at det foreligger et brudd på personopplysningssikkerheten ettersom det ble foretatt uhjemlede kredittsjekker. Etter oppfatning skulle bruddet vært meldt til Datatilsynet.

Selv om kredittvurderingene var uhjemlede har dere vurdert at avviket ikke er meldepliktig etter personvernforordningen artikkel 33, og dere har derfor ikke meldt inn avviket til oss tidligere. I vurderingen er det lagt vekt på at:

- antallet berørte er lavt
- det ikke er behandlet særlige kategorier personopplysninger;
- personopplysningene er underlagt streng tilgangsbegrensning;
- øvrige kopier av personopplysningene ble slettet eller kryptert:
- den berørte har fått informasjon om avviket; og
- det dreier seg om en opplysningskategori som dere regelmessig håndterer.

Dere skriver derimot at konklusjonen kunne blitt en annen dersom dere hadde funnet holdepunkter for at klagers påstand om deling av kredittopplysninger med tredjeparter hadde vært riktig.

I merknadene fremheves det at dere i tillegg la vekt på følgende forhold da det i løpet av våren ble avdekket ny kredittvurdering av klager:

- Datatilsynet ble skriftlig orientert om saken den 24. april 2020, 8. mai 2020 og 4. juni 2020, selv om korrespondansen ikke formelt ble benevnt avviksmelding eller liknende. I disse henvendelsene ble Datatilsynet oppfordret til å ta kontakt med dere.
- Kredittvurderingene innebar ikke innhenting av ytterligere personopplysninger enn de som allerede var innhentet. Antall berørte var følgelig fortsatt kun 1, dvs. et lavt antall.
- Kredittvurderingen 24. april 2020 ble lest i Bisnodes løsning den 24. april 2020, men ikke lastet ned eller distribuert, og skadepotensialet var følgelig lavt.
- Kredittvurderingene av aksjeselskapet innebar ingen innhenting av personopplysninger, og det er derfor fire kredittvurderinger som er relevante i forhold til meldeplikten.

4. Regelverkets krav

4.1 Særlig om behandlingsgrunnlag 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 (behandlingsgrunnlag). Når en virksomhet skal innhente kredittopplysninger om en enkeltperson eller enkeltpersonforetak er artikkel 6 nr. 1 bokstav f det relevante behandlingsgrunnlaget.

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[1] er videreført som gjeldende rett.

Den nye kredittopplysningsloven[2] 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 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.

4.2. 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 viktige interessen er for virksomheten, om behandlingen har offentlig interesse eller ivaretar en ideelle interesse som kommer flere til gode, se Artikkel 29-gruppens uttalelse («WP29»).[3]

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

---

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

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.

4.3. 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.

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-2006-2003 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.*

I PVN-2010-05 sier Personvernnemnda at det motsatte av «saklig behov» er «nysgjerrighet og kikkermentalitet».

4.4. Plikten til internkontroll
Etter personvernforordningen artikkel 24 plikter alle virksomheter å kunne påvise at de behandler personopplysninger i samsvar med loven. 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 må derfor kunne dokumentere at deres interne rutiner og prosesser ivaretar kravet om saklighet ved kredittvurdering. Rutinene skal beskrive når og hvordan kredittopplysninger skal innhentes og hvordan innsyn skal gis, og skal sikre at kredittvurderinger ikke innhentes uten at kravet om saklig behov er oppfylt.

Videre bør virksomheten også ha rutiner for håndtering av brudd på personopplysningssikkerheten for å sikre at man etterlever forordningens krav til å melde brudd til tilsynsmyndigheten.

4.5 Brudd på personopplysningssikkerheten
Personvernforordningen artikkel 33 fastsetter at den behandlingsansvarlige i utgangspunktet plikter å melde «brudd på personopplysningssikkerheten» til oss som tilsynsmyndighet

«Brudd på personopplysningssikkerheten» er definert i personvernforordningen artikkel 4 nr. 12 som:

> *...et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet,*

Det skal meldes fra uten ugrunnet opphold, og senest innen 72 timer etter behandlingsansvarlig har fått kjennskap til bruddet, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter.

5. Datatilsynets vurdering
5.1 Behandlingsgrunnlag for innhenting av kredittopplysninger
Det relevante behandlingsgrunnlaget for innhenting av kredittopplysninger om klager og klagers enkeltpersonforetak er personvernforordningen artikkel 6 nr. 1 bokstav f. Spørsmålet er om Innovasjon Norge hadde et lovlig behandlingsgrunnlag etter artikkel 6 nr. 1 bokstav f da dere innhentet kredittopplysninger om klager.

Det er i denne vurderingen kredittvurderingene av klager personlig og enkeltpersonforetak som er gjenstand for vurdering etter personvernforordningen. Kredittvurderingene av klagers aksjeselskap er ikke omfattet av regelverket ettersom det ikke regnes som personopplysninger etter loven.

Det første vilkåret som må være oppfylt for at behandling skal være lovlig er at dere hadde en «berettiget interesse» i å innhente opplysningene.

Kravet til «berettiget interesse» er i stor grad en videreføring av det samme kravet i den tidligere personopplysningsloven av 2000 § 8 første ledd, bokstav f. 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.

I henhold til merknadene har dere ytt et lån til en bedrift ved navn , og dere bemerker at det er offentlig kjent at klager har hevdet at daglig leder i har brutt en intensjonsavtale med klager. Dere skriver at saksbehandleren som var ansvarlig for tre av de fire kredittvurderingene har forklart at disse hadde sammenheng med den nevnte intensjonsavtalen. Dere har imidlertid selv konkludert med at kredittvurderingene ikke var saklig begrunnet og manglet behandlingsgrunnlag. Dere skriver at saksbehandleren er sagt opp fra stillingen som følge av dette. Vedrørende kredittvurderingen som ble gjennomført 24. april 2020 har dere forklart at klager ble kredittvurdert på grunn av en misforståelse hvor

saksbehandler trodde klager var en potensiell kunde. Dere har informert at arbeidstakeren er under arbeidsrettslig oppfølging som følge av dette.

Datatilsynet kan følgelig ikke se at det er godtgjort at det foreligger en berettiget interesse som kan begrunne de fire kredittvurderingene som er gjort av klager og enkeltpersonforetak, tvert imot fremstår ikke dette som omtvistet i saken.

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» og foreta den konkrete interesseavveiningen ettersom vår vurdering er at dere ikke hadde en berettiget interesse til å gjennomføre kredittvurderingen.

Konklusjonen er etter dette at Innovasjon Norge ikke hadde rettslig grunnlag etter artikkel 6 nr. 1 bokstav f for å behandle kredittopplysninger om klager personlig, innhentet 18. januar 2020, og enkeltpersonforetak, 8. januar 2020, 21. februar 2020 og 24. april 2020.

5.2 Plikten til internkontroll
Dere skriver i redegjørelsen at dere har skriftlige retningslinjer for innhenting av kredittopplysninger. Retningslinjene skal følges av finansieringsrådgiverne i all saksbehandling og det gis opplæring av nyansatte.

Det er ledelsens ansvar at man har tilstrekkelige rutiner, at man følger opp regelmessig at disse fungerer som tiltenkt og er godt kjent i virksomheten, jf. ansvarlighetsprinsippet i artikkel 5 nr. 2. Det er ikke tilstrekkelig å ha rutiner dersom disse ikke faktisk gjennomføres og etterleves i organisasjonen.

Den dagjeldende rutinen for kredittvurderinger datert 30. august 2017 er svært generelt formulert og viser til at det er en lav terskel for å kredittvurdere. Som PwC viser til i sin rapport er det ikke eksplisitt oppgitt når en ikke skal gjennomføre en kredittsjekk, eller minstekrav for at det kan gjennomføres kredittsjekk av privatpersoner. I styrenotat fra styremøte 29. mai 2020 kommer det fram at styret besluttet å følge opp disse merknadene og utbedre rutinene på dette punktet. De nye rutinene datert 24. juni 2020 er mer detaljerte og gir bedre veiledning til de ansatte.

Videre har PwC anbefalt at det innføres jevnlige gjennomganger av rutiner og praksis på området, at man har en periodisk gjennomgang av tilganger til å kredittvurdere, at man vurderer om tilganger skal være graderte ut fra den enkelte saksbehandlerens behov, samt at det ses på muligheten for å i større grad kunne etterprøve om kredittvurderingene er foretatt med hjemmel. Disse anbefalingene er det også besluttet å følge opp.

Dere skriver selv at saken har vist et behov for ytterligere tydeliggjøring av retningslinjene og at kunnskapen ikke har vært god nok. På denne bakgrunn anser vi det ikke hensiktsmessig å pålegge dere å utarbeide nye rutiner.

Vi legger til grunn at dere følger opp at de tiltakene som er besluttet fungerer og er tilstrekkelige for å forhindre lignende situasjoner. Det er viktig at organisatoriske og tekniske tiltak følges opp med god opplæring.

Til tross for at dere gjentar i merknadene at saken har avdekket at internkontrollen på området ikke har vært god nok, understreker dere at dere hadde internkontrolltiltak før de aktuelle kredittvurderingene ble foretatt. Disse kommentarene er gitt i forbindelse med artikkel 83 nr. 2 bokstav d. Vi vil kommentere dette ytterligere nedenfor.

5.3 Brudd på personopplysningssikkerheten
Når det gjelder hvor og når kredittvurderingene er utført, så anser vi ikke dette som et brudd på personopplysningssikkerheten, jf. artikkel 4 nr. 12. Vi er derimot av den oppfatning at kredittvurderingene utgjør et brudd på personopplysningssikkerheten ettersom det har skjedd en ulovlig tilgang til klagers personopplysninger, jf. artikkel 4 nr. 12.

Vi registrerer at Innovasjon Norge har vurdert om bruddet er meldepliktig etter artikkel 33, men kommet til at det ikke er det. Vi registrerer også at dere har rutiner for å håndtere brudd på personopplysningssikkerheten.

Av Skullerud m.fl. (ajourført versjon av kommentarutgaven til personvernforordningen, heretter omtalt som kommentarutgaven) fremgår det i tilknytning til artikkel 33:

> *Typiske konsekvenser som må vurderes i forbindelse med et sikkerhetsbrudd er om den registrerte mister kontroll over egne personopplysninger, blir utsatt for forskjellsbehandling, identitetstyveri eller -bedrageri, påføres økonomisk tap, får skadet sitt omdømme, mister fortrolighet om taushetsbelagte personopplysninger, eller medfører andre betydelige økonomiske eller sosiale ulemper for den berørte fysiske personen, jf. fortalepunkt 85.*
>
> *Ved vurderingen er det naturlig å ta hensyn til hva slags type sikkerhetsbrudd det er snakk om, herunder om sikkerhetsbruddet også medførte et brudd på andre bestemmelser i forordningen. Det er videre aktuelt å ta hensyn til hvilke kategorier personopplysninger som er berørt, graden av identifikasjon, og om det er snakk om et stort antall personopplysninger knyttet til den enkelte. Det kan også tas hensyn til antall registrerte som er berørt av sikkerhetsbruddet, og hvilke kategorier av registrerte det er snakk om.*[4]

I tillegg bemerkes det følgende i kommentarutgaven:

> *Det oppstår for det første meldeplikt dersom sikkerhetsbruddet medfører en behandling som er ulovlig, altså en behandling som er i strid med forordningens*

[4] Åste Marie Bergseng Skullerud, Rønnevik, Skorstad og Pellerud, *Personvernforordningen. Lovkommentar,* side 387. Juridika (kopiert 12. mai 2021)

bestemmelser. Dette vil typisk gjelde dersom sikkerhetsbruddet har medført en utlevering av personopplysninger som manglet rettslig grunnlag i forordningen art. 6.[5]

Det er imidlertid ikke nødvendig å melde bruddet til Datatilsynet dersom det sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter, jf. artikkel 33 nr 1.

Dere anfører prinsipalt at det ikke forelå meldeplikt etter artikkel 33 nr. 1. Dere skriver i denne anledning, blant annet, at det totalt dreide seg om fire kredittvurderinger med innhenting av personopplysninger, at antallet berørte var lavt og at dere hadde iverksatt mitigerende tiltak. I merknadene etterspør dere også en nærmere klargjøring fra Datatilsynet om når plikten inntrådte, samt at vi tar i betraktning Personvernrådet («EDPB») sine nye retningslinjer på området som ble vedtatt 14. januar 2021.

Ved spørsmålet om kredittvurderingene skulle ha blitt meldt til Datatilsynet i henhold til artikkel 33 nr. 1, må det skilles mellom de tre første kredittvurderingene (utført 18. januar 2020, 18. januar 2020, samt 21. februar 2020) og den fjerde kredittvurderingen (utført den 24. april 2020).

Først adresseres de tre første kredittvurderingene. I denne anledning må det vurderes om de tre første kredittvurderingene, utført uten behandlingsgrunnlag, sannsynligvis ikke ville medføre en risiko for fysiske personers rettigheter og friheter. I et slikt tilfelle vil det ikke være nødvendig å melde forholdet til Datatilsynet.

I veilederen til WP29 om brudd på personopplysningssikkerheten, sist revidert februar 2018, fremgår det at man skal blant annet vektlegge følgende i risikovurderingen etter artikkel 33:

> (...) *the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.*[6] (Egne uthevninger)

Kredittopplysninger er en type personopplysninger som er særlig beskyttelsesverdig, ettersom de er en sammenstilling av personopplysninger fra mange ulike kilder. En kredittvurdering vil vise detaljer om privatøkonomi, herunder eventuelle betalingsanmerkninger, frivillige pantstillelser og gjeldsgrad. Dette er private opplysninger som privatpersoner har en forventning ikke innhentes med mindre det er saklig begrunnet. Privatpersoner bør ha et særlig vern mot innhenting av kredittopplysninger.

I merknadene beskriver dere nærmere bakgrunnen for hvorfor de tre første kredittvurderingene ble gjennomført. Dere skriver at dere har ytt et lån til en bedrift ved navn

---

[5] Ibid side 386
[6] Guidelines on Personal data breach notification under Regulation 2016/679, side 25

og at det har vært offentlig kjent at klager har hevdet at daglig leder i har brutt en intensjonsavtale med klager. Dere forklarer at de tre første kredittvurderingene hadde sammenheng med denne intensjonsavtalen.

Klager kontaktet dere om i løpet av 2019. Klager var av den oppfatning at dere hadde opptrådt uredelig som følge av deres relasjon til .[7] Sett fra klagers perspektiv blir utsatt for gjentatte kredittvurderinger, som gir innsikt i meget omstendelige og private personopplysninger, av en aktør som tidligere har anklaget for å opptre uredelig.

Videre ble de to første kredittvurderingene utført rundt kl 22 på en lørdag, innenfor et veldig kort tidsrom. Kredittvurderingene ble gjort av klager personlig og enkeltpersonforetak. Innenfor et så kort tid har det formodningen sterkt imot seg at informasjonen som presenteres i Bisnode har endret seg, i tillegg vil begge søkene produsere praktisk talt identisk informasjon om klager ettersom kredittopplysninger om enkeltpersonforetak er direkte knyttet til eierens privatøkonomi. Til tross for at dere skriver i merknadene at dere ikke har klart å avdekke at søkene ikke var arbeidsrelatert, så fremstår handlingsmønsteret uansett som atypisk, da særlig sett i lys av at klager ikke hadde en relasjon til dere som gjorde det påregnelig at skulle bli kredittvurdert. At klager igjen blir søkt opp litt over én måned senere, rundt midnatt til lørdag, bidrar til å forsterke dette inntrykket.

Kombinasjonen av tidligere kritikk av dere, det faktum at kredittvurderinger er en type personopplysninger som er særlig beskyttelsesverdig og at handlingsmønsteret for øvrig fremstod som atypisk, skaper en særlig oppfordring til å reagere da dere innser at har blitt utsatt for urettmessige kredittvurderinger.

Dere skriver i merknadene at vurderingen etter artikkel 33 må tas i lys av formålet bak bestemmelsen, som dere skriver blant annet er Datatilsynets informasjonsbehov. Kommentarutgaven skriver at meldeplikten sørger for at tilsynsmyndigheten blir i stand til å vurdere om det er nødvendig å benytte sin kompetanse til å iverksette eller pålegge tiltak for å gjenopprette situasjonen og begrense skadevirkningen av sikkerhetsbruddet.[8]

I denne anledning vil de gjentatte urettmessige kredittvurderingene være en indikasjon på at det ikke er implementert tilfredsstillende internkontroll i den aktuelle virksomheten. Dette antyder også EDPB i sin veileder fra 2021, som i denne anledning skriver:

> *Data breaches are problems in and of themselves, but they are also symptoms of a vulnerable, possibly outdated data security regime, thus indicate system weaknesses to be addressed* (...) .[9]

En melding i henhold til artikkel 33 vil gi oss en foranledning til å undersøke forholdet nærmere, og dermed muligens avdekke, for eksempel, manglende internkontroll. Vi har derfor et informasjonsbehov i slike tilfeller. Dette gir oss mulighet til å sørge for at passende tiltak blir implementert, herunder sørge for at hverken den berørte eller andre fysiske personer

[7] Brev fra klager, 6. mai 2020, side 9
[8] Kommentarutgaven, side 385
[9] Guidelines 01/2021 on Examples regarding Data Breach Notification, 14 januar 2021, avsnitt 8

utsettes for lignende hendelser i fremtiden. I lys av størrelsen på virksomheten deres og volumet av kredittvurderinger som dere utfører gjør informasjonsbehovet seg særlig gjeldende.

På bakgrunn av momentene nevnt ovenfor skulle de aktuelle kredittvurderingene utført 18. januar, 18. januar og 21. februar ha blitt meldt til Datatilsynet i henhold til artikkel 33 nr. 1.

Dere viser for øvrig til at dere søkte råd hos Datatilsynets veiledningstjeneste den 8. april 2020. I telefonsamtalen med veiledningstjenesten skal dere ha mottatt støtte for deres syn om at forholdet ikke var meldepliktig etter personvernforordningen artikkel 33 nr. 1. I merknadene har dere vedlagt en e-post fra Ingrid Nilsen Leipsland til Håvard Kjærstad, sendt i etterkant av samtalen med veiledningstjenesten.

I henhold til vedlagt e-post ser det ut som veiledningstjenesten fikk et begrenset innsyn i sakens faktiske omstendigheter. Veiledningstjenesten fikk vite at det var gjennomført en kredittsjekk av én person ved to anledninger, at dere hadde underlagt opplysningene streng tilgangskontroll og at dere hadde gitt vedkommende informasjon. Det var tilsynelatende på denne bakgrunn veiledningstjenesten skal ha uttalt at det hørtes ut som situasjonen var under kontroll. Veiledningstjenesten fikk dermed, tilsynelatende, blant annet ikke innsikt i forhistorien deres med den som hadde blitt kredittvurdert, samt at internkontrollen deres på dette tidspunktet ikke var tilstrekkelig god. Det fremstår også som uklart om veiledningstjenesten fikk innsikt i hvem som ringte, og om vedkommende dere snakket med var klar over det store volumet av kredittvurderinger som dere utfører. Videre ønsker vi å bemerke at dere kontaktet Datatilsynets veiledningstjeneste på et sent tidspunkt. Kredittvurderingene ble utført den 18. januar 2020 og 21. februar 2020. Dere var imidlertid iallfall kjent med forholdet da Håkon Haugli, administrerende direktør i Innovasjon Norge, den 6. mars 2020 kontaktet klager for å beklage for kredittvurderingene.

Uansett er Datatilsynets veiledningstjeneste utelukkende ment for veiledning. Som Ingrid Nilsen Leipsland selv bemerker i e-posten, så saksbehandler ikke veiledningstjenesten. Det er den behandlingsansvarlige som er ansvarlig for de aktuelle vurderingene. Vi har derfor ikke, uavhengig av innholdet i samtalen, ansett kontakten med veiledningstjenesten som et forhold som endrer synet vårt på at hendelsene var meldepliktig.

Vedrørende den fjerde kredittvurderingen, utført den 24. april 2020, så ble denne gjennomført etter at dere hadde blitt innklagd til Datatilsynet for å ha gjennomført gjentatte urettmessige kredittvurderinger. Kredittvurderingen ble utført på et tidspunktet der dere hadde all foranledning til å sikre at ikke ytterligere urettmessige kredittvurderinger av klager skulle bli gjennomført. At det igjen blir utført en urettmessig kredittvurdering illustrerer at dere imidlertid ikke klarte å sikre dette. Dette ledet til at dere den 5. mai 2020 stengte ned alle tilganger til systemet for å få kontroll. Dere har for øvrig fortalt at den aktuelle kredittvurderingen ble utført av en ansatt uten egen tilgang. At det ble utført en ny kredittvurdering under disse forholdene innebærer at den fjerde kredittvurderingen også utgjorde et brudd på personopplysningssikkerheten som skulle ha blitt meldt inn til Datatilsynet i henhold til artikkel 33.

I merknadene er deres subsidiære anførsel at meldeplikten uansett må anses oppfylt gjennom henvendelsene deres datert 24. april 2020, 8. mai 2020 og 4. juni 2020. Denne anførselen vil bli vurdert i det følgende.

For de tre første kredittvurderingene kommer ikke spørsmålet om henvendelsene oppfyller minimumsvilkårene i artikkel 33 nr. 3 bokstav a til d på spissen. Årsaken til dette er at fristen i artikkel 33 nr. 1 uansett ikke er overholdt. Ledelsen i virksomheten hadde iallfall kjennskap til at kredittvurderingene hadde blitt urettmessig gjennomført i starten av mars 2020. Brudd på personopplysningssikkerheten skal bli meldt til Datatilsynet uten ugrunnet opphold. Begrunnelsen for hvorfor forholdet ikke ble meldt innen tidsfristen i artikkel 33 ser ut til å være at dere var av den oppfatning at hendelsene ikke utgjorde et meldepliktig forhold. Dere brøt derfor plikten deres etter artikkel 33 nr. 1 ved å ikke melde ifra om de urettmessige kredittvurderingene som hadde blitt gjennomført 18. januar 2020, 18. januar 2020 og 21. februar 2020.

Angående den fjerde kredittvurderingen kan ikke brevet deres datert 24. april 2020 anses som en melding i artikkel 33 nr. 1 forstand. Til tross for at kredittvurderingen den 24. april 2020 ble utført før dere sendte brev til oss, skrev dere ingenting om kredittsjekken. Først den 8. mai 2020 gav dere informasjon om at en ny kredittvurdering hadde blitt utført den 24. april 2020.

Det sentrale vurderingstemaet blir derfor om henvendelsen deres 8. mai 2020 kan anses til å være en melding i henhold til artikkel 33 nr. 1.

Den 8. mai 2020 sendte dere oss en e-post. I denne e-posten fremgikk det at dere avdekket at det var foretatt en ny kredittvurdering av klager, samt at dere ikke hadde nødvendig oversikt over hvilke ansatte som hadde tilgang til kredittopplysningsverktøyet som brukes. Dere skrev at dere skulle foreta ytterligere undersøkelser og ville komme tilbake til oss dersom det skulle vise seg at dette utgjorde et meldepliktig brudd etter artikkel 33. Vedlagt til e-posten var en pressemelding som dere hadde sendt ut, samt en e-post fra administrerende direktør til de ansatte.

Ettersom dere skriver i e-posten at dere vil ta en vurdering av om hendelsen utgjør et meldepliktig forhold indikerer dette at dere ikke selv oppfattet e-posten som en henvendelse som avbrøt fristen i artikkel 33 nr. 1. Imidlertid beskriver e-posten arten av bruddet på personopplysningssikkerheten, kontaktopplysninger sammen med en klar oppfordring om å ta kontakt for mer informasjon, samt hvilke tiltak som er iverksatt. Det fremgår også forutsetningsvis hvilke konsekvenser dette bruddet på personopplysningssikkerheten kan ha. På denne bakgrunn anser vi e-posten med vedlegg som en melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten i henhold til artikkel 33.

Det er derfor nødvendig å ta stilling til om meldingen ble sendt inn tidsnok, jf. artikkel 33 nr. 1. Dere har informert oss om at dere ble klar over den fjerde kredittvurderingen den 5. mai 2020.[10] I lys av at den fjerde kredittvurderingen ble oppdaget 5. mai 2020 og meldt til

[10] Brev fra Innovasjon Norge, 10. august 2020, side 2

Datatilsynet den 8. mai 2020, anser vi meldeplikten i artikkel 33 nr. 1 til å være overholdt for kredittvurderingen utført 24. april 2020.

Vi har på denne bakgrunn konkludert med at dere brøt meldeplikten ved å ikke melde inn kredittvurderingene som ble utført den 18. januar, 18. januar og 21. februar 2020, men at dere overholdt meldeplikten deres for kredittvurderingen som ble utført den 24. april 2020.

Datatilsynet har imidlertid forståelse for at vurderingen av om en hendelse er meldepliktig kan være utfordrende. Datatilsynet har lagt vekt på at dere har foretatt en konkret vurdering av om det var nødvendig å sende inn avviksmelding. Dere har i denne anledning presentert relevante argumenter og gitt oss en nærmere begrunnelse for hvorfor dere var av den oppfatning at forholdet ikke var meldepliktig. Dere har, blant annet, påpekt at dere ikke hadde holdepunkter for at disse opplysningene ville bli spredt videre til tredjeparter, at antallet berørte var lavt, at det ikke handlet om særlige kategorier opplysninger, og at den berørte hadde fått informasjon om avviket.[11]

Til tross for at Datatilsynet er av den oppfatning at de urettmessige kredittvurderingene skulle blitt meldt til oss har vi valgt, som i varselet, å ikke ilegge dere overtredelsesgebyr for brudd på artikkel 33.

Imidlertid har vi vektlagt at dere ikke underrettet oss om hendelsen, noe som har blitt ansett som en skjerpende omstendighet etter artikkel 83 nr. 2 bokstav h. Dette vil bli adressert ytterligere nedenfor.

6. Overtredelsesgebyr

6.1 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, 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. 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 menneskerettighetskonvensjonen.

For foretak er skyldvurderingen særegen. I Forvaltningsloven § 46 første ledd heter det:

[11] Brev fra Innovasjon Norge, 24 april 2020, punkt 2

> «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 uttaler departementet 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 gjort objektivt.»

6.2 Vurdering av om overtredelsesgebyr skal ilegges
Adgangen til å ilegge overtredelsesgebyr er gitt som et virkemiddel for å sikre effektiv etterlevelse og håndhevelse av personopplysningsloven. Det følger av forordningens artikkel 83 nr. 1 at hver tilsynsmyndighet skal sørge for at ilegging av overtredelsesgebyr i hvert enkelt tilfelle er «virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende».

Ved vurdering 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 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 tidligere bemerket er kredittopplysninger en type personopplysninger som er særlige beskyttelsesverdig. En kredittvurdering er en sammenstilling av personopplysninger fra mange ulike kilder, og viser et tall som angir sannsynligheten for at en person eller et enkeltpersonforetak vil betale en fordring. Den vil også vise detaljer om enkeltpersonforetakets økonomi, herunder eventuelle betalingsanmerkninger, frivillige pantstillelser og gjeldsgrad. Kredittopplysninger om enkeltpersonforetak er direkte knyttet til eierens privatøkonomi. Privatpersoner har en forventning om at det ikke innhentes kredittopplysninger med mindre det er saklig begrunnet i forholdet til virksomheten.

Klager har ikke hatt et forhold til virksomheten som gjorde det påregnelig at dere skulle behandle kredittopplysninger om vedkommende. Likevel har og enkeltpersonforetaket blitt kredittvurdert fire ganger. Tre ganger av samme finansieringsrådgiver, og i tillegg ble kredittvurdert av en saksbehandler som ikke hadde eget brukernavn og passord til Bisnodes systemer.

Klager ble kredittvurdert sent på kvelden utenfor vanlig arbeidsuke, henholdsvis to ganger lørdag 18. januar rundt kl. 22 og fredag 21. februar rundt midnatt. Dette framstår som noe unaturlig, og kan isolert sett indikere at de har skjedd utenfor arbeidstid. ble igjen kredittvurdert 24, april 2020, noe som var en misforståelse som oppstod da en ansatt ikke leste en tilsendt e-post godt nok.

I merknadene skriver dere imidlertid at det moderne arbeidslivet medfører at det ikke lenger er uvanlig med arbeid på kveldstid. Dere skriver at dere har undersøkt omstendighetene nærmere og ikke funnet grunnlag for at kredittvurderingene 18. januar 2020 og 21. februar 2020 ikke ble innhentet i arbeidsøyemed.

Datatilsynet er enig i at dagens moderne arbeidsliv kan medføre at man jobber på andre tider av døgnet enn før. Vi utelukker ikke at den ansatte har arbeidet utenfor ordinær arbeidstid i dette tilfellet. Imidlertid må tidspunktene som kredittvurderingene ble utført på ses i lys av klagers tidligere kontakt med dere. Som tidligere bemerket henvendte klager seg til dere fordi opplevde at dere opptrådte uredelig som følge av at dere finansierte en aktør som var i konflikt med. Denne aktøren var som i henhold til merknadene er samme aktør som forårsaket at dere kredittvurderte klager. A bli urettmessig kredittvurdert gjentatte ganger av en aktør man har anklaget for å opptre uredelig, på meget uvanlige tidspunkt, øker graden av belastning for klager og dermed alvorlighetsgraden for øvrig.

I merknadene skriver dere at dere forstår at mange vil oppleve det belastende å bli kredittvurdert, og at dette var en av grunnene til at dere var raskt ute med tiltak for å redusere personvernbelastningen i februar 2020. Imidlertid mener dere at Datatilsynet må ta i betraktning:

- At dere har siden første henvendelse fra klager mottatt et hundretalls e-poster fra klager,
- At det har vært stor pågang i form av telefonsamtaler og SMSer til ansatte, ledelse og styremedlemmer på nærmest alle døgnets tider,
- At klager flere ganger har selv offentliggjort det faktum at er blitt kredittvurdert, og at i denne konteksten har behandlet personopplysninger om ansatte hos dere på en uakseptabel måte som resulterte i at dere den 29. april 2020 besluttet å anmelde klager for hensynsløs atferd.

At dere har opplevd situasjonen som belastende blir ikke vektlagt ved vurdering av overtredelsesgebyr. Dersom dere mener at klager har brutt personopplysningsregelverket må dette bli adressert i sin egen sak. Vi har for øvrig ikke vektlagt den offentlige oppmerksomheten som saken har fått som følge av klagers uttalelser til media i en skjerpende retning.

I merknadene skriver dere at til tross for at kredittvurderingene manglet behandlingsgrunnlag så skyldes ikke kredittvurderingene «kikkermentalitet». Innhentingen av kredittopplysningene har sin årsak i menneskelige feilvurderinger, som har blitt fulgt opp av dere i et arbeidsrettslig

spor. Dere ber Datatilsynet om i vurderingen av alvorlighetsgrad ta hensyn til at virksomheters internkontroll aldri vil være en garanti mot menneskelige feil.

Vi har forståelse for at virksomheters internkontroll aldri vil være en garanti mot menneskelige feil. Imidlertid er det erkjent i denne saken at internkontrollen deres ikke var tilstrekkelig. Dette ledet til at dere i mai 2020 måtte stenge ned alle tilganger til systemet for å få kontroll. Følgelig, på tidspunktet da de fire kredittvurderingene ble utført, var ikke internkontrollen god nok. Det er derfor ikke tale om en situasjon hvor internkontrollen var god, men menneskelige feil allikevel medførte sikkerhetsbrudd.

Angående nysgjerrighet og kikkermentalitet har Datatilsynet ikke konkludert med, eller for øvrig vektlagt, at kredittvurderingene ble utført på grunn av «kikkermentalitet». Referansen til «kikkermentalitet» er ment å kaste lys på hva Personvernnemnda anser til å være det motsatte av «saklig behov» og dermed bidra til å kartlegge ytterpunktene som vurderingen må tas innenfor.

Vi er for øvrig enig med deres kommentarer, om at personopplysningens kontekst er relevant for å vurdere den konkrete risikoen for klagers rettigheter og friheter. Herunder viser dere til at undersøkelsene deres indikerer at det ikke er grunn til å tro at det ble innhentet andre typer personopplysninger om klager, og at risikoen besto følgelig i at et lite antall medarbeidere hadde behandlet opplysninger knyttet til en person. Dere har også vist til at personen ikke er en del av en sårbar gruppe. Dere mener at Datatilsynet ikke har lagt tilstrekkelig vekt på dette.

Vi har imidlertid tatt disse forholdene i betraktning. Som vi vil gå ytterligere inn på nedenfor utgjør overtredelsesgebyret dere har blitt ilagt rundt 0,08 prosent av deres driftsinntekter i 2019. Gebyret er derfor betydelig lavere enn hva personvernforordningen artikkel 83 nr. 5 gir Datatilsynet kompetanse til å ilegge en sak som dette. Årsaken til dette er, blant annet, slike forhold.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

De tre første kredittvurderingene skjedde uten at det var gjennomført tilstrekkelig vurdering av det rettslige grunnlaget for behandlingene og dere hadde ikke implementert tilfredsstillende internkontroll, noe som medfører en åpenbar risiko for at det kunne skje brudd på regelverket. Vedrørende den fjerde kredittvurderingen ble denne utført fordi den ansatte ikke leste e-posten ordentlig, og vedkommende utførte kredittvurderingen ved hjelp av lånt brukertilgang. Dette karakteriseres som uaktsomt.

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

I merknadene skriver dere at det ble iverksatt mitigerende tiltak den 27. februar 2020 ved å underlegge kredittopplysningene meget streng tilgangsbegrensning og besørge sletting av kopier. Etter dere den 5. mai 2020 ble kjent med at brukertilganger til

kredittopplysningsverktøyet ikke var ajourført ble tilgangen til verktøyet stengt for alle ansatte påfølgende dag. Dere mener at dette må trekke i formildende retning.

I WP29 sine retningslinjer om overtredelsesgebyr fra 2017 skrives det, blant annet, følgende om dette punktet:

> *This provision acts as an assessment of the degree of responsibility of the controller after the infringement has occurred. It may cover cases where the controller/processor has clearly not taken a reckless/ negligent approach but where they have done all they can to correct their actions when they became aware of the infringement.*[12]

WP29 gir et eksempel på et slikt tilfelle:

> (...) *timely action taken by the data controller/processor to stop the infringement from continuing or expanding to a level or phase which would have had a far more serious impact than it did.*[13]

Dere har iverksatt tiltak, herunder stengte dere brukertilgangen i mai 2020. Dere hadde på dette tidspunktet informasjon som gjorde det klart at dere manglet tilstrekkelig kontroll over kredittvurderingene som ble utført.

Imidlertid, til tross for at dere var kjent med at virksomheten hadde foretatt gjentatte kredittvurderinger av klager og at det var en pågående prosess med Datatilsynet, klarte dere ikke å forhindre at en ny kredittvurdering ble gjennomført den 24. april 2020. Dette var i tillegg en kredittvurdering som ble utført av en medarbeider uten egen tilgang. Dere klarte derfor ikke å reagere på en måte som begrenset skadeomfanget. Det er på denne bakgrunn ikke grunnlag for å vektlegge tiltakene eller reaksjonen deres for øvrig i en særlig formildende retning i denne 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*

Ansvarlighetsprinsippet forutsetter en sterk forankring av regelverket i virksomheters ledelse, jf. personvernforordningen artikkel 5 nr. 2.

Dere skriver at kredittvurderinger er en ordinær del av deres saksbehandling i finansieringssaker og at dere utfører mange kredittsjekker i løpet et kalenderår. Vi forstår det slik at kredittvurderinger er et svært praktisk arbeidsverktøy.

---

[12] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, side 12 til 13
[13] Ibid side 13

Vi vil understreke at kredittvurderinger medfører et betydelig inngrep i privatlivet til de som blir kredittvurdert. Dere er en stor offentlig aktør som er avhengig av tillit i befolkningen for å kunne utføre samfunnsoppdraget på en god måte. Dette tilsier at ledelsen bør utarbeide og implementere gode rutiner for hvordan kredittvurderinger skal benyttes. Rutiner må følges opp og justeres om de ikke fungerer som tiltenkt.

Dere skriver at tilganger til å foreta kredittvurderinger er blitt delt mellom ansatte i virksomheten. Klager ble blant annet kredittvurdert av noen med en videreformidlet tilgang. Dette gir inntrykk av at dere ikke har fulgt opp at retningslinjene for kredittvurderingen faktisk har fungert og vært tilstrekkelige. Dette trekker i skjerpende retning.

I merknadene erkjenner dere at internkontrollen på området for kredittvurderinger ikke har fungert godt nok. Imidlertid skriver dere at til forskjell fra annen norsk tilsynspraksis fra Datatilsynet i 2021 så hadde dere iverksatt en rekke internkontrolltiltak før de aktuelle kredittvurderingene ble foretatt. Dere mener derfor at dere ikke burde bli dømt like strengt som de andre sakene der det var fullstendig fravær av tekniske og organisatoriske tiltak.

Dere viser i denne anledning blant annet til at dere hadde følgende internkontrolltiltak før de aktuelle kredittvurderingene ble tatt:

- Retningslinjer for bruk av kredittvurderinger var nedfelt i den interne håndboken for alle som behandler finanseringssaker (finanseringshåndboken)
- Internrevisors (PwC) rapport om bruk av kredittvurderinger fra 22. mai 2020 viste at det generelt var god kjennskap til finanseringshåndboken og til retningslinjer for bruk av kredittvurderinger hos dere. Intervjuer med ansatte i selskapet viste at de hadde en klar oppfatning om hva som anses som misbruk av kredittvurderinger.
- Selv om det ikke eksplisitt var oppgitt i finanseringshåndboken når en ikke skulle gjennomføre en kredittvurdering, eller angitt minstekrav for kredittvurderinger av privatpersoner, var disse retningslinjene supplert med øvrige krav til opptreden som gjelder for deres ansatte, derunder det etiske rammeverket som blant annet stiller krav til behandling av personopplysninger i samsvar med grunnleggende personvernhensyn
- Innhenting av kredittopplysninger var en del av den opplæring som ble gitt til saksbehandlere av finanseringssaker.

Datatilsynet er enig i at dere hadde internkontrolltiltak før kredittvurderingen ble gjennomført. For øvrig må kravene som stilles til internkontrollen til en virksomhet ses i lys av behandlingsaktivitetene til virksomheten og risikoen forbundet med behandlingen, jf. artikkel 24. Dere gjennomfører et betydelig antall kredittvurderinger hvert år. Det er derfor gode grunner til å stille strenge krav til deres internkontroll og rutiner.

Som vi vil gå ytterligere inn på nedenfor må årlig omsetning og inntekter til virksomheten tas i betraktning ved fastsettelse av overtredelsesgebyr. Med et slikt utgangspunkt er det grunnlag for å mene at dere har fått en mildere reaksjon sammenlignet med andre saker som angikk

kredittvurderinger, ikke strengere som dere antyder i merknadene. Vi viser i denne anledning til sakene som angår kredittvurderinger som har blitt publisert på vår nettside i løpet av 2021.

I Aquateknikk-saken utgjorde overtredelsesgebyret ca 1 prosent av virksomhetens estimerte omsetning i 2020. I Lindstrand Trading-saken gjorde de gjeldende at det ikke var midler til å dekke gebyret, og de la frem regnskapstall fra proff.no som viste at selskapet ikke hadde noen omsetning i 2018 eller 2019. Selskapet fikk et overtredelsesgebyr på kr 100 000 i lys av virksomheten var registrert med aksjekapital på kr 800 000 og at det tilsynelatende var aktivitet på nettbutikken deres. I Gveik-saken hadde selskapet omsetning på kr 49 000 i 2017, mens i 2019 var driftsinntektene på kr 0 og årsresultatet på minus kr 30 000. Overtredelsesgebyret ble på kr 75 000.

For øvrig viser vi også til Personvernnemndas avgjørelse i PVN-2020-21. I denne saken hadde Datatilsynet ilagt et overtredelsesgebyr på kr 150 000. Driftsresultatet til virksomheten i 2019 var på kr 1,9 millioner. Overtredelsesgebyret utgjør derfor mellom 7 og 8 prosent av driftsresultatet deres. Selskapet fikk ikke medhold hos Personvernnemnda i at dette var et urimelig høyt gebyr, idet Personvernnemnda uttalte:

> *Nemnda er enig med Datatilsynet i at det skal ilegges et overtredelsesgebyr og finner etter en vurdering av de ulike momentene at et gebyr på 150 000 kroner i alle fall ikke er for høyt.* (egne uthevninger)

Vi mener at reaksjonen dere har blitt ilagt ikke er uforholdsmessig eller for øvrig urimelig, dette til tross for at dere hadde noe internkontrolltiltak før de aktuelle kredittvurderingene. Vi viser som ovenfor til at dere har blitt ilagt et overtredelsesgebyr som utgjør rundt 0,08 prosent av deres driftsinntekter i 2019, i dette vedtaket.

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

I merknadene skriver dere at dere ikke tidligere har blitt ilagt gebyr for overtredelse av personvernlovgivningen. Dette forholdet er hensynstatt ved utmåling av overtredelsesgebyret.

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

I merknadene skriver dere at samarbeidet dere har hatt med oss for å opplyse saken ikke har blitt vektlagt tilstrekkelig ved fastsettelse av overtredelsesgebyrets størrelse.

Som nevnt i varselet til vedtak har vi imidlertid lagt til grunn at dere har selv redegjort for at kredittvurderingene ble foretatt uten rettslig grunnlag, og at dere for øvrig har bidratt til sakens opplysning. Dette forholdet har derfor ikke blitt ansett som en skjerpende omstendighet, og er etter vårt syn tilstrekkelig hensynstatt ved fastsettelse av overtredelsesgebyret.

> *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*

I merknadene skriver dere, i deres kommentar til bokstav h, blant annet:

- At bruddet på personopplysningssikkerheten ikke er meldepliktig etter artikkel 33 nr. 1.
- At meldeplikten uansett anses oppfylt gjennom henvendelsene datert 24. april 2020, 8. mai 2020 og 4 juni 2020.
- At det for øvrig ikke er grunnlag for at «grad av underretning» kan vektlegges i skjerpende retning.

Spørsmålet om underrettelse i personvernforordningen artikkel 83 nr. 2 bokstav h er separat fra hvorvidt hendelsen er meldepliktig etter artikkel 33 nr. 1. Det sentrale spørsmålet er hvordan tilsynsmyndighetene fikk kjennskap til overtredelsen.

Vi fikk kjennskap til de tre første kredittvurderingene ved klagers henvendelse datert 17. april 2020. Kontakten deres med veiledningstelefonen 8. april kan ikke anses til å være en slik underrettelse ettersom veiledningstelefonen gir generell hjelp og skal ikke saksbehandle.

Til tross for at spørsmålet om underrettelse er separat fra meldeplikten etter artikkel 33 nr. 1, er vår oppfatning at de tre første kredittvurderingene var meldepliktig etter artikkel 33, jf. artikkel 4 nr. 12. Dette medfører at dere hadde en særlig oppfordring til å underrette oss om hendelsen.

Vedrørende den fjerde kredittvurderingen utført 24. april 2020 så har vi, som nevnt, lagt til grunn at dere overholdt meldeplikten i artikkel 33 nr. 1 ved deres henvendelse 8. mai 2020. Imidlertid var det ikke dere som først informerte oss om hendelsen. Vi ble underrettet om denne kredittvurderingen i brev fra klager datert 6. mai 2020.

WP29 har i sine retningslinjer fra 2017 også gitt uttrykk for at selv i de tilfeller der den behandlingsansvarlige oppfyller sin forpliktelse til å melde fra om hendelsen vil ikke dette i seg selv anses som en formildende omstendighet:

> *The controller has an obligation according to the Regulation to notify the supervisory authority about personal data breaches. Where the controller merely fulfils this*

> *obligation, compliance with the obligation cannot be interpreted as an attenuating/ mitigating factor.*[14]

Imidlertid beskriver kommentarutgaven, side 698, en noe motstridende tilnærming:

> *Det kan argumenteres for at overtrederens egen varsling bør virke formildende også i de tilfellene hvor det foreligger en meldeplikt til Datatilsynet etter forordningen art. 33. Det vises her til at en streng sanksjonspraksis i slike tilfeller kan svekke tilliten mellom tilsynsmyndighetene og de behandlingsansvarlige, og i verste fall medføre at sikkerhetsbrudd ikke meldes som forutsatt.*

Vi har på denne bakgrunn vektlagt at vi ble underrettet av overtredelsene av klager, noe som trekker i skjerpende retning. Vi har imidlertid kun ansett dette som en skjerpende omstendighet for de tre første kredittvurderingene.

Ettersom dere overholdt meldeplikten for den fjerde kredittvurderingen har vi valgt å ikke anse dette forholdet som en skjerpende omstendighet, selv om det var klager som underrettet oss først om denne kredittvurderingen også. Vi har imidlertid heller ikke ansett dette som en formildende omstendighet, noe som er i tråd med Datatilsynets egen praksis.[15]

Samlet trekker artikkel 83 nr. 2 bokstav h i skjerpende retning.

> *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*

Som nevnt ble det utført gjentatte kredittvurderingene under omstendigheter som økte belastningen for klager. I tillegg framgår det at dere ikke hadde full kontroll på hvem som hadde tilganger til å foreta kredittvurderinger. Dette er kritikkverdige momenter som taler for at overtredelsesgebyr ilegges.

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

6.3 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.

---

[14] Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, side 15

[15] Sak 20/01790, Vedtak om ileggelse av overtredelsesgebyr – COOP FINNMARK SA, side 13. Tilgjengelig på våre nettsider: https://www.datatilsynet.no/aktuelt/aktuelle-nyheter-2021/vedtak-om-overtredelsesgebyr-til-coop-finnmark/

Vi har ved utmåling av gebyrets størrelse lagt vekt på de samme vurderingsmomentene som ble gjennomgått ovenfor. Datatilsynet viser derfor til vurderingene gjort ovenfor, og at disse samlet taler for et gebyr av en viss størrelse.

Virksomhetens økonomiske evne er som nevnt også av betydning, selv om det ikke er aktuelt å utnytte 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.

Av kommentarutgaven, side 701, 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.*

Dere mottar midler til drift over statsbudsjettet. Det kommer fram av resultatregnskapet for 2019 at dere hadde driftsinntekter på kr 1 297 252 000. Ut fra regnskapet, samt karakteren av bruddet på personvernforordningen i saken, har vi kommet frem til at et overtredelsesgebyr på kr 1 000 000 er riktig.

Som omtalt ovenfor har dere i merknadene gitt uttrykk for at dere oppfatter overtredelsesgebyret som urimelig høyt. Dere viser, blant annet, til bruddets alvorlighetsgrad, det konkrete skadepotensialet, belastningen for klager, samt antall berørte.

Vi har imidlertid tatt hensyn til disse forholdene ved utmåling av overtredelsesgebyret. I denne anledning ønsker vi igjen å understreke at overtredelsesgebyret utgjør rundt 0,08 prosent av deres årlige driftsinntekter. Vi minner om at brudd på personvernforordningen artikkel 6 kan medføre sanksjoner i form av overtredelsesgebyr på opptil 20 millioner euro eller opptil 4 prosent av den årlige globale årsomsetningen i det forutgående regnskapsår, jf. artikkel 83 nr. 5. Gebyret som ilegges i denne saken, er således helt i det nederste sjiktet av hva forordningen foreskriver for slike regelverksbrudd.

7. Inndrivelse av overtredelsesgebyr

Overtredelsesgebyret forfaller til betaling fire uker etter at vedtaket er endelig, jf. personopplysningsloven § 27. Vedtaket er tvangsgrunnlag for utlegg. Inndrivelse av kravet vil bli gjennomført av Statens innkrevingssentral.

8. Klageadgang

Dere kan klage på vedtaket. En eventuell klage må sendes oss **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.

9. Offentlighet

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.

Dersom dere har spørsmål i saken kan dere kontakte Carl Emil Bull-Berg på telefon: 22 39 69 77

Med vennlig hilsen

Jørgen Skorstad
avdelingsdirektør, jus

Carl Emil Bull-Berg
juridisk rådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

Kopi til: