Datatilsynet

BRABANK ASA
Postboks 4126 Sjølyst
0217 OSLO

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

Deres referanse	Vår referanse	Dato
	20/02376-5	28.05.2021

Vedtak om overtredelsesgebyr - Melding om avvik - BRABANK ASA (tidl. Easybank ASA)

1. Innledning

Vi viser til vårt varsel om vedtak om overtredelsesgebyr av 7. april 2021 til BRABANK ASA («BRABANK»).

Personvernombudet i BRABANK har bekreftet i telefonsamtale med Datatilsynets saksbehandler 19. mai 2021 at selskapet ikke har merknader til varselet, og at selskapet godtar det varslede gebyret.

Tilsynet fatter derfor vedtak om overtredelsesgebyr i samsvar med varselet, og vår begrunnelse følger nedenfor.

2. Vedtak om ileggelse av overtredelsesgebyr

1. *Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i ilegges BRABANK ASA, org.nr. 986 144 706, et overtredelsesgebyr på kr 400 000 for:*
    - *Brudd på personvernforordningen artikkel 24 nr. 1, ved at det ikke er gjennomført egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i tråd med forordningen, og*
    - *Brudd på personvernforordningen artikkel 32 nr. 1 og 2, ved at det ikke er gjennomført egnede tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå.*

Vår hjemmel for å ilegge overtredelsesgebyr er personvernforordningen artikkel 58 nr. 2 bokstav i.

Oppfyllelsesfristen følger av vedtakets pkt. 6.

3. Beskrivelse av avviket

Datatilsynet mottok avviksmelding fra Easybank ASA (nå: BRABANK ASA) 6. september 2019. Ifølge avviksmeldingen kunne noen kunder se andre kunders låneforhold da banken lanserte «Min Side» 3. september 2019. «Min Side» er en løsning hvor kundene får oversikt over sitt låneengasjement.

Avviket oppstod ved hyppig navigering på siden, grunnet et problem med «verifisering av sessions per bruker».

På spørsmål om den nærmere årsaken til at avviket oppstod, opplyser BRABANK ASA i redegjørelsen datert 29. mai 2020 at de ikke har klart å gjenskape feilen i test. [redacted]

Ifølge avviksmeldingen kunne enkelte kunder se andre kunders personnummer, navn, telefonnummer, e-post, lånenummer, restlån, status på lån, utbetalingskonto, informasjon om fakturaer, og opplysninger om eventuelle forsikringsforhold. Forsikringsproduktene er tilknyttet lånet.

I redegjørelsen datert 29. mai 2020, skriver BRABANK ASA at personnummer likevel ikke lå tilgjengelig for andre kunder. Kundene kunne heller ikke se hvem de finansielle opplysningene tilhørte.

Dersom kunden fulgte en lenke for å verifisere kontaktopplysninger, kunne de få opp kontaktopplysningene til andre kunder. Disse opplysningene ville ikke nødvendigvis være tilknyttet lånet de hadde fått innsyn i.

BRABANK ASA har funnet ut at én kunde fikk opp en annen kundes adresseinformasjon og minst to kunder fikk opp feil låneinformasjon.

På spørsmål fra Datatilsynet, opplyser BRABANK ASA at risikoen for de registrertes rettigheter og friheter ble vurdert som lav, ettersom kundene ikke kunne gjøre endringer i løsningen, og informasjonen som ble presentert ikke var av sensitiv karakter. BRABANK ASA har ikke dokumentasjon på denne vurderingen.

På spørsmål fra Datatilsynet, skriver banken at løsningen ble testet i perioden mai 2019 til august 2019 i deres testmiljø. Deretter ble den verifisert/testet i et internt miljø som peker mot produksjonsdatabasen. Ved lansering sendte banken ut påloggingsinformasjon til et mindre utvalg kunder (ca. 500). Av disse var det 91 kunder som logget seg inn før utrullingen ble reversert.

BRABANK ASA oppdaget avviket ved at en kunde tok kontakt kort tid etter lansering, og opplyste om at saldoen og betalingsplanene ikke samsvarte med hennes lån. BRABANK ASA

stengte «Min Side» umiddelbart etter dette, ti minutter etter lanseringen. De 91 kundene som var pålogget i tidsrommet kl. 11:35-11:45 var potensielt rammet av avviket.

Som avhjelpende tiltak er det i avviksmeldingen oppgitt at utbedring av problemet er under arbeid og omfattende testing vil bli foretatt før nettsiden blir satt i produksjon igjen. Videre at banken vil legge inn en ekstra verifisering i systemet. Deretter gjennomgå alle handlinger som er utført på «Min Side» av de berørte kundene for å kvalitetssikre gyldigheten av endringene.

Av redegjørelsen fremgår det at BRABANK ASA har byttet ut datatilkobleren [redacted] Dersom det oppstod et avvik ville kunden få en feilmelding og det ville bli logget i deres database.

Løsningen ble så testet, og deretter relansert for et mindre utvalg av kundene. Etter 14 dager uten feil ble løsningen lansert for alle kundene. Etter 6 måneders drift har det ikke blitt loggført noen nye feil.

Banken har informert de 91 kundene om avviket på SMS og e-post, og informert om avhjelpende tiltak.

4. Nærmere om personopplysningslovens krav

4.1. Den «behandlingsansvarliges» ansvar

Den «behandlingsansvarlige» er den som bestemmer formålet med behandlingen og hvilke midler som skal benyttes, jf. 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.

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.

4.2. Grunnprinsippene for behandling av personopplysninger

De grunnleggende prinsippene for behandling av personopplysninger følger av personvernforordningen artikkel 5 nr. 1. Vi viser til artikkel 5 nr. 1 bokstav a, b, c og f:

1. *Personopplysninger skal*

a) behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),

b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenelig med disse formålene (...) («formålsbegrensning»),

c) være adekvate, relevante og begrenset til det som er nødvendig for formålene de behandles for («dataminimering»), (...)

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

Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at personvernprinsippene overholdes, jf. artikkel 5 nr. 2.

4.3. Sikkerhet ved behandlingen

Kravene til personopplysningssikkerhet er nærmere regulert i artikkel 32. Her følger det:

1. Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige og databehandleren gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen, herunder blant annet, alt etter hva som er egnet,

a) pseudonymisering og kryptering av personopplysninger,

b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene, (...)

d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

2. *Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av (...) ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet».*

4.4. Datatilsynets korrigerende myndighet

Datatilsynets korrigerende myndighet følger av personvernforordningen artikkel 58 nr. 2.

Datatilsynet har blant annet kompetanse til å ilegge overtredelsesgebyr og utstede irettesettelse ved overtredelser.

Ifølge fortalepunkt 148 til personvernforordningen, bør det ved overtredelser av forordningen «ilegges sanksjoner, herunder overtredelsesgebyr, i tillegg til eller i stedet for egnede tiltak som tilsynsmyndigheten pålegger» i henhold til forordningen. Ved mindre overtredelser kan det gis en irettesettelse i stedet for et overtredelsesgebyr.

I vurderingen av om overtredelsesgebyr skal ilegges, skal Datatilsynet legge vekt på momentene i artikkel 83 nr. 2 bokstav a til k.

5. Datatilsynets vurdering

5.1. Behandlingsansvarlig

Banken har selv sendt inn avviksmeldingen etter artikkel 33, som pålegger den behandlingsansvarlige å melde avvik til Datatilsynet. Saken gjelder behandling av personopplysninger gjennom lansering av «Min Side», en påloggingstjeneste som etter det opplyste tilhører Easybank ASA (nå: BRABANK ASA).

Basert på dette legger vi til grunn at BRABANK ASA bestemte formålet med og middelet for behandlingen, slik at banken er «behandlingsansvarlig» etter artikkel 4 nr. 7.

5.2. Den behandlingsansvarliges ansvar, jf. artikkel 24

Spørsmålet er om BRABANK ASA ved lansering av «Min Side» gjennomførte egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen.

Som nevnt under punkt 4 er integritet og konfidensialitet et grunnleggende prinsipp etter personvernforordningen. Artikkel 5 nr. 1 bokstav f bestemmer at personopplysninger må behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot utilsiktet tap, ødeleggelse eller skade.

Ved vurderingen av hvilke tiltak som er egnet, skal den behandlingsansvarlige 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.

«Min Side» er en løsning som tilbyr kundene oversikt over sitt låneengasjement. Basert på redegjørelsene fra BRABANK ASA, legger vi til grunn at løsningen ville vise kundens lånedetaljer, herunder saldo på lån og betalingsplan(er).

Lanseringen av «Min Side» innebar altså behandling av kundenes finansielle opplysninger.

Disse opplysningene er ikke særlige kategorier av personopplysninger etter personvernforordningen artikkel 9. Opplysningene kan imidlertid fortsatt være av sensitiv karakter for de registrerte. I motsetning til eksempelvis inntekter, er ikke finansielle opplysninger offentlig tilgjengelig informasjon. Datatilsynets personvernundersøkelser har også vist at opplysninger om privatøkonomi oppleves som særlig beskyttelsesverdig.[1] Hele 89 % mente dette ifølge Datatilsynets personvernundersøkelse for 2019/2020.[2]

Ifølge hjemmesidene, tilbyr banken alminnelige banktjenester, men også forbrukslån og refinansiering. Etter vår vurdering kan særlig opplysninger om den type gjeld føles sårt for mange, noe også en rapport fra SIFO underbygger.[3]

Vi er derfor ikke enig med BRABANK ASA i at opplysningenes karakter talte for lav risiko for de registrertes rettigheter og friheter. Tvert imot mener vi opplysningenes karakter taler for en høyere alvorlighetsgrad, slik at tiltakene må vurderes deretter.

Videre innebar «Min Side» i første omgang en behandling av 500 kunders personopplysninger, før løsningen skulle rulles ut til resten av kundebasen. Gjennom løsningen ville BRABANK ASA altså behandle personopplysningene til et stort antall registrerte.

Både artikkel 24 og artikkel 32 oppstiller en plikt til å foreta en risikovurdering. Denne skal blant annet ta hensyn til risikoen en planlagt behandling av personopplysninger utgjør for fysiske personers rettigheter og friheter.

Risikovurderingen danner grunnlaget for hvilke tiltak i henhold til artikkel 24 og 32 som er egnet, og det danner grunnlaget for vurderingen av om den behandlingsansvarlige må gjennomføre en konsekvensutredning (DPIA) etter artikkel 35. Risikovurderingen er altså styrende for den behandlingsansvarliges internkontroll og informasjonssikkerhet.

Etter vår vurdering talte behandlingens art, omfang og sammenhengen den skulle utføres i, for en grundig vurdering av tiltak for å sikre og påvise at behandlingen ville bli utført i samsvar med forordningen.

Etter vår vurdering kan ikke BRABANK ASA fremlegge dokumentasjon eller på annen måte påvise at de gjennomførte nødvendige vurderinger i henhold til artikkel 24 og 32.

Basert på dette er vår foreløpige konklusjon at banken ikke har overholdt sitt ansvar etter artikkel 24 nr. 1.

---

[1] Se Datatilsynet, Personvernundersøkelsen 2013/2014, https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvernundersokelsen-2013-delrapporter/ (besøkt 14.1.2021) og Datatilsynet, Personvernundersøkelsen 2019/2020, https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvernundersokelsen-20192020/ (besøkt 14.1.2021)

[2] Datatilsynet, Personvernundersøkelsen 2019/2020, https://www.datatilsynet.no/regelverk-og-verktoy/rapporter-og-utredninger/personvernundersokelser/personvernundersokelsen-20192020/ (besøkt 14.1.2021)

[3] Jf. https://www.oslomet.no/forskning/forskningsnyheter/stor-forbrukslan-skam-i-norge (besøkt 14.1.2021)

5.3. Sikkerhet ved behandlingen etter artikkel 32

Det neste spørsmålet er om BRABANK ASA ved lansering av «Min Side» gjennomførte egnede tekniske og organisatoriske tiltak for å oppnå et egnet sikkerhetsnivå i henhold til artikkel 32.

Risikovurdering

Ved vurderingen av hvilke tiltak som er egnet, skal den behandlingsansvarlige ta hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål, og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for de registrertes rettigheter og friheter. Integritet- og konfidensialitetsprinsippet er et grunnleggende prinsipp etter personvernforordningen, jf. artikkel 5 nr. 1 bokstav f.

Risikoen for fysiske personers rettigheter og friheter er styrende for hvilke sikkerhetstiltak de behandlingsansvarlige må gjennomføre før de setter i gang en ny behandlingsaktivitet. Dette fremgår av artikkel 32 nr. 1 og nr. 2.

BRABANK ASA kan imidlertid ikke dokumentere risikovurderingen, og opplyser at de vurderte risikoen som lav. Banken viser til at opplysningene som kundene skulle få tilgang til gjennom løsningen ikke var av sensitiv karakter.

Som nevnt er vi ikke enige i bankens vurdering om at opplysningenes karakter talte for lav risiko. Ettersom finansielle opplysninger ville bli behandlet i løsningen, talte behandlingens art for en høyere alvorlighetsgrad, slik at tiltakene måtte vurderes deretter.

Videre vil utrulling av en ny løsning som «Min Side» alltid være forbundet med risiko for tekniske feil og sikkerhetsbrudd, herunder risiko for brudd på konfidensialitet, integritet og tilgjengelighet.

Vi mener derfor at sannsynligheten for avvik talte for en reell risiko for de registrertes rettigheter og friheter.

Behandlingens omfang er andre momenter i vurderingen av hvor omfattende sikkerhetstiltakene må være, jf. artikkel 32 nr. 1.

Som nevnt innebar løsningen i første omgang en behandling av personopplysningene til 500 av bankens kunder. Det høye antallet registrerte mener vi også talte for en høy grad av personopplysningssikkerhet.

Artikkel 32 oppstiller en plikt til å gjennomføre en risikovurdering, uansett hva slags type personopplysninger det er snakk om, og uansett om det er mulig å gjøre endringer i løsningen eller ikke. Plikten til å gjennomføre risikovurdering er regulert flere steder i forordningen. Dette viser hvor grunnleggende slike vurderinger er for ivaretakelse av

personopplysningssikkerheten. Vi finner imidlertid ikke BRABANK ASA sitt svar på spørsmål om risikovurdering betryggende, og mener det er grunn til å stille spørsmål ved om risikoen ble vurdert, og om det i så fall forelå en forsvarlig vurdering.
Egnede sikkerhetstiltak

Ifølge artikkel 32, skal den behandlingsansvarlige iverksette egnede sikkerhetstiltak med utgangspunkt i risikoene som har blitt avdekket i risikovurderingen.

BRABANK ASA testet løsningen i perioden mai 2019 til august 2019 i eget testmiljø. Deretter verifiserte/testet de løsningen i et internt miljø som peker mot produksjonsdatabasen. Ved lansering sendte de ut påloggingsinformasjon til et mindre utvalg kunder (ca. 500).

Etter vår vurdering er banken lite konkret i beskrivelsen av hvordan testingen ble gjennomført, og den har ikke lagt ved dokumentasjon, eksempelvis testprotokoll, for å påvise hvilke tiltak som ble gjennomført før lanseringen. Dette mener vi kan indikere mangelfull testing. At avviket oppstod samme dag som løsningen ble lansert for et utvalg av kundene, kan også underbygge at testingen var utilstrekkelig.

Det fremgår av avviksmeldingen at avviket oppstod ved hyppig navigering på siden. Vi informerer om viktigheten av testing og ulike testmetoder i vår veiledning om innebygget personvern.[4] Der nevner vi også sesjonshåndtering, som banken opplyser om at har vært en av årsakene til avviket.

Vi bemerker at de finansielle opplysningene som har vært tilgjengeliggjort for andre kunder i saken ikke har vært knyttet til navn eller andre kontaktopplysninger. Vår vurdering at det er tilfeldigheter som gjorde at bruddet på personopplysningssikkerheten ikke førte til at også kontaktopplysninger ble tilgjengeliggjort for uvedkommende, ettersom løsningen ikke har blitt testet godt nok. Tilstrekkelige tekniske tiltak i form av testing er en grunnleggende forutsetning for å avdekke sårbarheter som kan føre til brudd på konfidensialitet som i denne saken.

Etter vår foreløpige vurdering ville tilstrekkelig testing ha avdekket feilene i løsningen. Tilstrekkelig testing og avdekking av feil før lanseringen kunne ført til at banken ble satt i stand til å iverksette egnede sikkerhetstiltak, og dermed unngått avviket.

Vi kan derfor ikke se at BRABANK ASA kan ha gjennomført tilstrekkelige sikkerhetstiltak før lansering, sett opp mot momentene som beskrevet ovenfor.

Konklusjon

Basert på ovennevnte, konkluderer vi med at risikovurderingen var mangelfull, at BRABANK ASA ikke foretok en forsvarlig vurdering av egnede tekniske og organisatoriske tiltak, og at de dermed ikke oppnådde et egnet sikkerhetsnivå sett opp mot risikofaktorene.

[4] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-med-innebygd-personvern/test/

Etter vår foreløpige konklusjon foreligger det derfor brudd på artikkel 32 nr. 1 og 2.

5.4. Vurdering av korrigerende tiltak

Datatilsynets korrigerende myndighet følger av personvernforordningen artikkel 58 nr. 2.

Avhengig av omstendighetene i hvert enkelt tilfelle skal overtredelsesgebyr ilegges i tillegg til eller i stedet for øvrige sanksjoner nevnt i artikkel 58 nr. 2 bokstav a) - h) og j), jf. artikkel 83 nr. 2 første punktum.

Ifølge fortalepunkt 148 til personvernforordningen kan det ved mindre overtredelser gis en irettesettelse i stedet for et overtredelsesgebyr. Ved alvorlige overtredelser er altså overtredelsesgebyr den primære sanksjonsformen.

I samsvar med Høyesteretts praksis (jf. Rt. 2012 side 1556) legger vi til grunn at overtredelsesgebyr er å anse som straff etter den europeiske menneskerettighetskonvensjonen artikkel 6. Det kreves derfor klar sannsynlighetsovervekt for lovbrudd for å kunne ilegge gebyr.

I vurderingen av om overtredelsesgebyr skal ilegges, skal Datatilsynet legge vekt på momentene i artikkel 83 nr. 2 bokstav a til k. Vi vil her vurdere momentene løpende.

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

Bruddet på personopplysningssikkerheten er et resultat av manglende tekniske og organisatoriske tiltak som sørger for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet og integritet, jf. forordningen artikkel 32. Prinsippet om konfidensialitet og integritet er grunnleggende etter personvernforordningen, jf. artikkel 5 nr. 1 bokstav f.

Etter vår vurdering fremstår det som om banken tilsidesatte grunnleggende sikkerhetsprinsipper ved mangelfulle utredninger og tiltak før lansering av løsningen. Vi kan ikke se at BRABANK ASA gjorde en forsvarlig risikovurdering og utredning av sikkerhetstiltak, dersom den i det hele tatt foretok slike vurderinger. Dette trekker i retning av at overtredelsen var alvorlig.

Videre innebar løsningen behandling av opplysninger som vi mener det er naturlig å oppfatte som beskyttelsesverdig informasjon. Opplysninger om privatøkonomi, spesielt opplysninger om forbrukslån, oppleves av mange som opplysninger av svært privat art. Behandlingsansvarlige må derfor være særlig aktsomme ved behandling av slike opplysninger, selv om det ikke dreier seg om særlige kategorier av personopplysninger. Banken ser imidlertid ut til å ha undervurdert dette, noe vi også mener trekker i skjerpende retning.

Karakteren og alvorlighetsgraden av overtredelsen taler altså for ileggelse av overtredelsesgebyr.

Vi ser også på varigheten av overtredelsen. BRABANK ASA stanset tilgangen til «Min Side» umiddelbart etter at de ble gjort oppmerksom på avviket. Sikkerhetsbruddet varte fra kl. 11:35 til 11:45. At banken handlet umiddelbart fører til at varigheten ikke utgjør et skjerpende moment i saken.

Omfanget av skaden de registrerte har lidd trekker ikke i spesielt skjerpende retning, ut fra opplysningene banken har kommet med. Kunder skal ikke ha fått tilgang til identifiserbare opplysninger om andre kunders finansielle situasjon. Imidlertid kunne kunder få tilgang til andre kunders kontaktopplysninger, som er identifiserbart.

Ifølge avviksmeldingen var 91 personer berørt av avviket, da dette var antall innloggede under sikkerhetsbruddet. Løsningen ble imidlertid rullet ut for 500 av kundene, og samtlige av disse ble dermed utsatt for risiko for brudd på konfidensialitet. Etter vår vurdering er det derfor 500 som ble berørt av overtredelsen.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Etter vår vurdering skulle BRABANK ASA ha gjennomført grundigere og dokumenterbar risikovurdering samt utredning av egnede sikkerhetstiltak. Basert på sakens opplysninger fremstår det som om banken bagatelliserte hvilke vurderinger de måtte gjennomføre før de registrerte kunne få tilgang til løsningen. Banken utsatte de registrerte for en risiko ved å lansere løsningen uten tilstrekkelig risikovurdering og tiltak. Sannsynligheten for avvik må derfor ha vært synlig for banken, og vi vurderer det som uaktsomt av banken å ikke iverksette bedre egnede tekniske tiltak for å avhjelpe denne risikoen slik personvernforordningen artikkel 32 krever.

Dette taler for at overtredelsesgebyr bør ilegges.

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

BRABANK ASA stanset tilgangen til «Min Side» umiddelbart etter at en kunde kontaktet dem og informerte om avviket. Ifølge banken iverksatte de sterkere sikkerhetstiltak før de lanserte løsningen igjen. Etter seks måneders drift har de ikke mottatt henvendelser om avvik.

Datatilsynet har ikke grunnlag for å vurdere om de avhjelpende tiltakene var tilstrekkelige. Vi ser imidlertid at banken handlet raskt da de ble gjort oppmerksom på avviket, noe som kan ha begrenset skadeomfanget. Dette trekker i formildende 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 har konkludert med at banken ikke gjennomførte tilstrekkelige tekniske og organisatoriske tiltak i henhold til artikkel 32. Videre vi at det foreligger brudd på artikkel 24, som nettopp regulerer den behandlingsansvarliges ansvar. Som nevnt tilsidesatte banken grunnleggende sikkerhetsprinsipper og undervurderte risikoen ved behandlingen. Det bør være alminnelig kjent at risikovurdering er et grunnleggende utgangspunkt for arbeid med sikkerhetstiltak i nye løsninger.

Ettersom banken ikke har gjort det som må forventes ut fra behandlingens art og omfang, mener vi graden av ansvar taler for ileggelse av overtredelsesgebyr.

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

Datatilsynet kjenner ikke til tidligere overtredelser.

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

Vi kan ikke se at dette momentet er relevant.

g) kategoriene av personopplysninger som er berørt av overtredelsen

Særlige kategorier av personopplysninger skal ikke være berørt av avviket. Banken skulle imidlertid behandle finansielle opplysninger om de registrerte, noe vi mener er en type personopplysninger som må behandles med særlig aktsomhet. Som nevnt er opplysninger om privatøkonomi noe som de registrerte opplever som særlig beskyttelsesverdig, og informasjon om forbrukslån oppleves som svært privat.

Basert på redegjørelsene fra banken er det imidlertid ikke sikkert at disse opplysningene var direkte identifiserbare da de ble gjort tilgjengelig for uvedkommende. På den andre siden synes dette i tilfelle å bero på tilfeldigheter, og banken tok etter vår vurdering ikke god nok høyde for risikoen for at finansielle opplysninger i deres behandlingssystemer kunne bli utsatt for konfidensialitetsbrudd.

Kategoriene av personopplysninger som er berørt av overtredelsen taler derfor for ileggelse av overtredelsesgebyr.

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

Vi fikk kunnskap om overtredelsen gjennom avviksmelding fra BRABANK ASA. Ifølge retningslinjer fra Artikkel 29-gruppen, vedtatt av Personvernrådet («EDPB»), er det ikke en formildende omstendighet at den behandlingsansvarlige etterlever sin meldeplikt.[5]

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 med hensyn til samme saksgjenstand.

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

Vi finner ikke dette momentet relevant for saken.

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

Vi har ikke konstatert hvorvidt BRABANK ASA har oppnådd noen økonomiske fordeler, eller unngått tap direkte eller indirekte som et resultat av overtredelsen.

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

5.5. Overtredelsesgebyrets størrelse

I utmålingen av gebyret skal momentene i punkt 5.4 ovenfor tillegges vekt, jf. artikkel 83 nr. 2. Gebyret skal i hvert enkelt tilfelle være virkningsfullt, stå i et rimelig forhold til overtredelsen og virke avskrekkende, jf. artikkel 83 nr. 1.

Redegjørelsen ovenfor viser at karakteren og alvorlighetsgraden, grad av ansvar og type personopplysninger som ble berørt, trekker i skjerpende retning.

I formildende retning trekker det at banken handlet umiddelbart da de ble gjort oppmerksom på avviket, og dermed kan ha begrenset skadeomfanget.

Vi ser også hen til at kundene ikke skal ha fått innsyn i direkte identifiserende opplysninger om andres privatøkonomi ved avviket, og vektlegger dette i formildende retning.

På den andre siden har mangelfulle rutiner ofte som konsekvens at risikoen for feil øker. I dette tilfellet var det manglende eller mangelfull risikovurdering og vurdering av egnede tiltak før lansering av en ny løsning som ville innebære behandling av personopplysninger i større

[5] Jf. Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, side 15.

omfang. Saken reiser grunnleggende sikkerhetsspørsmål, og signaleffektene må anses å være til stede.

Ettersom gebyret i hvert enkelt tilfelle skal være virkningsfullt og virke avskrekkende, vil vi også se hen til virksomhetens økonomi.

BRABANK ASA er i 2019 registrert med inntekter på kr 271 380 000 og årsresultat på kr 86 180 000.

Etter en helhetsvurdering av saken har vi kommet til at et overtredelsesgebyr på **kr 400 000** anses riktig.

6. Klagerett

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.

7. Innsyn og offentlighet

Dere har rett til innsyn i sakens dokumenter (jf. forvaltningsloven § 18). Vi vil også 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.

Dersom dere har spørsmål om saken, kan dere kontakte juridisk rådgiver Ole Martin Moe på telefon 22 39 69 59.

Med vennlig hilsen

Jørgen Skorstad
avdelingsdirektør

Ole Martin Moe
juridisk rådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer