Hvorfor SATS-avgjørelsen er relevant for din virksomhet

Petter Bjerke
Partner, Faggruppeleder personvern og immaterialrett

Julie Ullerud Lind
Advokatfullmektig

Sofie Roscher Conley
Jurist

Den 6. februar 2023 utstedte Datatilsynet et overtredelsesgebyr på 10 millioner kr til SATS for brudd på personvernforordningen, GDPR. Datatilsynets konklusjon er ikke overraskende, men saken er en påminnelse om hvor viktig det er både å ha rutiner for håndtering av forespørsler om informasjon, innsyn og sletting, og å etterleve disse. Saken viser også den praktiske konsekvensen av å mangle dokumentasjon på behandlingsgrunnlag før personopplysninger behandles, og hvorfor virksomheter bør behandle personvernerklæringer som ferskvare.

I denne artikkelen oppsummerer vi saken og begrunner hvorfor avgjørelsen er relevant for *alle* virksomheter som behandler personopplysninger om sine kunder.

Kort om saken

6. februar 2023 ble det klart at Datatilsynet opprettholder det varslede gebyret på 10 millioner kroner for brudd på flere bestemmelser i GDPR. Saken har sin bakgrunn i fire individuelle klager rettet til Datatilsynet fra både tidligere og nåværende SATS-medlemmer i perioden 2018-2021. Klagene gjaldt ulike forhold, men saksforholdene hadde flere likheter, som medførte at Datatilsynet behandlet klagene samlet.

Samlet sett omhandlet klagene manglende ivaretakelse av SATS-medlemmenes rett til informasjon, innsyn og sletting, og manglende behandlingsgrunnlag. Det endelige gebyret gjenspeiler imidlertid også forhold utover den enkelte klage, da Datatilsynets samlede behandling av klagene avdekket bredere, mer systematiske svakheter internt i SATS med hensyn til etterlevelse av GDPR. Dette fikk betydning i utmålingen.

I det følgende gjennomgår vi de ulike kravene reist av de fire klagerne, og Datatilsynets vektlegging av forhold utover de konkrete klagene.

1) Krav om innsyn

Klager nr. 1 og 2 sendte innsynsbegjæring til SATS i 2018 og 2019, med forespørsel om informasjon om behandlingen eller kopi av personopplysningene som ble behandlet. Den ene innsynsbegjæringen ble aldri besvart, mens den andre ble besvart uten at SATS oppga all lovpålagt informasjon. Forholdene utgjorde brudd på SATS' forpliktelser etter GDPR artikkel 12(3) og artikkel 15, til å gi den registrerte all lovpålagt informasjon uten ugrunnet opphold og senest innen én måned etter at innsynsbegjæring er mottatt.

2) Krav om sletting

I 2019, fremsatte både klager nr. 2 og 3 krav om sletting av personopplysninger etter endt medlemskap, som følge av utestengelse fra SATS, og i 2021, fremsatte klager nr. 4 krav om sletting av treningslogg. Klager nr. 4 trakk samtidig tilbake sitt samtykke for fremtidig behandling av disse opplysningene.

Etter GDPR artikkel 12(3) og artikkel 17(1)(a), er SATS forpliktet til å foreta sletting uten ugrunnet opphold og senest innen en måned, dersom personopplysningene *«ikke lenger [er] nødvendige for formålet som de ble samlet inn eller behandlet for*». Bestemmelsen er en referanse til lagringsbegrensningsprinsippet i artikkel 5(1)(e). Lagringsvurderingen krever at SATS, *før* personopplysninger samles inn, har angitt et spesifikt og berettiget *formål* med behandlingen. Formålet danner altså utgangspunktet for lagringsvurderingen.

SATS besvarte slettebegjæringen fra klager nr. 2 og 3 med at alle personopplysninger ville bli slettet, med unntak av visse opplysninger (navn, fødselsdato og bilde for klager nr. 3 og «selve medlemsprofilen» for klager nr. 2) som ville bli lagret i 60 måneder. Utestengelsen fra treningssenteret for de to klagerne var henholdsvis 24 og 12 måneder, og SATS informerte ikke klagerne om *hvorfor* det var nødvendig å lagre opplysningene i flere år etter utestengelsen opphørte.

Datatilsynet foretok en selvstendig vurdering av hva som var formålet med lagringstiden og lovligheten av lagringstiden på 60 måneder, og bemerket følgende:

- Formålet med lagringstiden var ikke kommunisert til klagerne i sletteforespørslene, og lå heller ikke tilgjengelig på SATS' hjemmesider eller i brukervilkårene. Formålet ble først kommunisert overfor Datatilsynet, og ble endret underveis i dialogen: i første omgang begrunnet SATS lagringstiden med *«å kunne forhindre det utestengte medlemmet fra å benytte seg av SATS' tjenester i løpet av utestengelsesperioden»*, men ved varsel om gebyr omformulerte SATS formålet til *«å kunne behandle opplysningene i forbindelse med utestengelsen*». Slik endring av formål er i strid med GDPR artikkel 5(1)(a), og Datatilsynet tok derfor utgangspunkt i den første formålsangivelsen i sin vurdering av lagringstiden.
- En lagringstid på 60 måneder er ekstraordinært lang og i strid med lagringsbegrensningsprinsippet i artikkel 5(1)(e). Herunder uttalte Datatilsynet at behandling av personopplysninger, for å forhindre det utestengte medlemmet fra å benytte SATS' tjenester i løpet av utestengelsesperioden på 12 og 24 måneder, ikke nødvendiggjør en lagringstid på 60 måneder.

Datatilsynet konkluderte med at det forelå brudd på SATS' plikt til å slette opplysningene etter GDPR artikkel 12(3) og artikkel 17(1)(a).

Overfor klager nr. 4, hadde SATS besvart slettebegjæringen med at treningsloggen ville bli slettet innen 6 måneder i tråd med deres personvernerklæring, og begrunnet lagringstiden med *beskyttelse av SATS-ansatte og smittesporing under pandemien*. SATS bestred også slettebegjæringen med henvisning til at det forelå *lovlig formål for behandlingen og utsatt sletting*, og viste til behandlingsgrunnlagene *nødvendig for å oppfylle en avtale* (artikkel 6(1)(b) *og berettiget interesse* (artikkel 6(1)(f)).

Etter en konkret vurdering av lagringstiden, konkluderte Datatilsynet med at det forelå brudd på SATS plikt til å slette opplysningene etter GDPR artikkel 12(3) og artikkel 17(1)(a). Det ble vist til følgende:

- De anførte behandlingsgrunnlagene som kunne ha begrunnet fortsatt lagring, var ikke lovlige (se under).
- En lagringstid på 6 måneder for treningshistorikk, av hensyn til gjennomføring av smittesporing, fremstår *uberettiget* og *uproporsjonalt*. En slik lagringstid burde samsvare med dokumentert inkubasjonstid og karantenekrav etter Covid-19-forskriften, som på tidspunktet var 14 dager karantene og 30 dagers lagringstid av opplysninger. Lagringstid på 6 måneder var følgelig langt utenfor.

3) Manglende behandlingsgrunnlag for behandling av treningslogg:

Ved behandlingen av klage nr. 4, oppdaget Datatilsynet svakheter i SATS angitte behandlingsgrunnlag for treningsloggen. Kravet til behandlingsgrunnlag innebærer at all behandling av personopplysninger må ha rettslig grunnlag for å være lovlig. GDPR artikkel 6 oppstiller seks alternative rettslige grunnlag.

Datatilsynet foretok en selvstendig vurdering av alle de anførte behandlingsgrunnlagene i saken, og konkluderte med at det ikke forelå behandlingsgrunnlag for SATS til å behandle medlemmets treningslogg etter GDPR artikkel 6.

i. Vurdering av SATS' generelle brukervilkår som behandlingsgrunnlag

Etter GDPR artikkel 6(1)(b) foreligger lovlig behandlingsgrunnlag dersom «*behandlingen er nødvendig for å oppfylle en avtale som den registrerte er part i*».

SATS viste til at behandlingen av treningslogg var nødvendig for å oppfylle SATS' generelle brukervilkår, som hadde følgende ordlyd:

«Medlemmet samtykker til at SATS lagrer treningshistorikk med det formål å kunne følge opp Medlemmets aktivitet og tilrettelegge Medlemmets treningsopplegg. (...) Medlemmet har rett til innsyn i sin treningshistorikk og kan kreve å få denne slettet. SATS skal bekrefte mottak av melding om sletting.»

Datatilsynet bemerket for det første at ordlyden i vilkårene indikerer at behandlingsgrunnlaget her hviler på *samtykke*, og ikke oppfyllelse av avtalen. For det andre, anså Datatilsynet vilkårene i artikkel 6(1)(b) uansett ikke oppfylt. Det ble vist til retningslinjer fra European Data Protection Board («EDPB») og praksis fra EU-domstolen, som angir at behandlingsgrunnlaget ikke kan benyttes med mindre behandlingen av personopplysninger er *strengt nødvendig* for å levere tjenestene etter avtalen. Selv om det ikke fremgår eksplisitt av Datatilsynets avgjørelse, er det avgjørende for vurderingen de *tjenestene som faktisk leveres av SATS*, og ikke hva som står i kontrakten.

Anvendt på det konkrete tilfellet, uttalte Datatilsynet at det ikke var nødvendig å behandle treningsloggen for at SATS skal kunne levere sine tjenester til medlemmet i henhold til brukervilkårene (som etter Datatilsynets vurdering hovedsakelig var tilgang til treningssenterets fasiliteter). Standpunktet ble underbygget ved at medlemmet, etter brukervilkårene, når som helst kunne kreve treningsloggen slettet, hvilket ikke ville vært mulig dersom treningsloggen var *nødvendig* for å levere avtalte tjenester.

ii. Vurdering av samtykke som behandlingsgrunnlag

Etter GDPR artikkel 6(1)(c) foreligger lovlig behandlingsgrunnlag dersom den registrerte har «*samtykket*» til behandlingen. For å være gyldig, må samtykket være «*frivillig, spesifikk, informert og utvetydig*» og avgitt *før* behandlingen utføres, jf. artikkel 4(11).

Etter Datatilsynets vurdering er det ikke tilstrekkelig å innlemme samtykket i brukervilkårene, dersom dette skal benyttes som behandlingsgrunnlag. Vurderingen er i tråd med retningslinjer fra EDPB, hvor det presumeres at samtykket ikke er frivillig avgitt dersom det ikke holdes adskilt fra avtalen. Bakgrunnen er at virksomhetens tjenester ikke kan gjøres betinget av at kunden samtykker til behandling av sine personopplysninger, jf. GDPR artikkel 7(4). Manglende frivillighet medførte dermed at det ikke forelå et gyldig samtykke som kunne utgjøre behandlingsgrunnlaget for SATS.

iii. Vurdering av berettiget interesse som behandlingsgrunnlag

Etter GDPR artikkel 6(1)(f) foreligger lovlig behandlingsgrunnlag dersom «*behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige*».

Datatilsynet avfeide dette behandlingsgrunnlaget uten nærmere vurdering, med henvising til at grunnlaget verken var nevnt i personvernerklæringen eller i brukervilkårene. Tvert om vurderte Datatilsynet at SATS' egne henvising til dette behandlingsgrunnlaget var et tegn på uklarhet internt i SATS vedrørende behandlingsgrunnlaget, hvilket underbygget konklusjonen om at det ikke forelå et lovlig behandlingsgrunnlag for treningsloggen.

4) SATS' håndtering av klagene viser systematisk svakhet i SATS' interne rutiner

Sett i sammenheng, bemerket Datatilsynet at SATS' håndtering av de fire henvendelsene ga uttrykk for en bredere, mer systematisk svakhet internt i SATS. Slik DLA Piper vurderer det, ble det særlig lagt vekt på følgende omstendigheter

- Samtlige forespørsler ble ikke besvart innen en måned, hvilket i seg selv er et brudd på fristen fastsatt i GDPR artikkel 12(3).
- SATS fulgte ikke opp egne sletterutiner. Selv om klager nr. 2 og 3 ble informert om at opplysninger utover navn, fødselsdag og bilde ville bli slettet innen 30 dager, ble opplysningene ikke slettet før to år senere. Tilsvarende ble ikke klager nr. 4 sine opplysninger slettet etter 6 måneder.
- Informasjon om lagringen av opplysninger i 60 måneder ved utestengelse var ikke tilgjengelig i brukervilkårene, påSATS' offentlige kanaler eller på annet vis. Denne informasjonen skulle vært gitt til *alle* medlemmer på tidspunktet for innsamling av personopplysninger. SATS innvendte i denne forbindelse at lagringstiden til opplysninger om ekskluderte medlemmer vil variere fra sak til sak og dermed vanskelig kan

angis på helt generelt grunnlag. Datatilsynet aksepterte innvendingen, men uttalte at medlemmene likevel som et minimum må få informasjon om at visse personopplysninger lagres ved utestenging og hvilke omstendigheter som avgjør denne lagringstiden. At klagerne først fikk informasjon om lagringen av opplysningene etter innsendt klage, utgjorde dermed et brudd på åpenhetsprinsippet i artikkel 5(1)(a).
- SATS sin personvernerklæring av 2021 oppfylte ikke informasjonskravene i GDPR artikkel 12 og 13. Det ble særlig vektlagt at SATS ikke kommuniserte hvilket behandlingsgrunnlag de konkrete behandlingene baserer seg på. Dette skal kommuniseres tydelig for hver enkelt behandling.

De overnevnte punktene viser at det forelå flere brudd på GDPR utover de konkrete rettighetsbestemmelsene. Særlig tydelig er at SATS, på tidspunktet for klagene, manglet tiltak og rutiner for å sikre at medlemmene personvernrettigheter ivaretas og etterleves. Ettersom slike svakheter påvirker rettighetene til så å si alle SATS-medlemmer (om lag 700 000), fikk det betydelig utslag ved utmålingen av gebyret.

Proporsjonalt gebyr eller «betydelig overreaksjon»?

I henhold til GDPR kan Datatilsynet, for overtredelser av denne type, ilegge virksomheter et gebyr på opptil 20 000 000 euro eller 4% av den samlede globale årsomsetningen i forutgående regnskapsår (der det høyeste beløpet skal anvendes).

Datatilsynet tok utgangspunkt i SATS sin omsetning i 2021 på 3 247 millioner kroner. Fire prosent av denne omsetningen er lavere enn 20 000 000 euro, og dermed ble målestokken 20 000 000 euro. **Et overtredelsesgebyr på 10 millioner kr utgjør ca. 5 % av maksimalt gebyr, og 0,3 % av SATS sin omsetning.**

Datatilsynet begrunnet gebyrets størrelse i en rekke momenter, blant annet:

- Bruddene isolert sett ikke er de mest alvorlige og har ikke hatt alvorlig eller betydelig innvirkning på den enkelte, men det er likevel snakk om flere brudd på rettigheter og forpliktelser som ligger i kjernen av den fundamentale rettigheten til databeskyttelse, hvilket taler i skjerpende retning.
- Varigheten av flere av bruddene var betydelige, og SATS forholdt seg passive selv etter gjentatt kontakt og oppfølgning.
- Sakene ga samlet sett uttrykk for bredere, mer systematiske svakheter internt i SATS. Et selskap på størrelsen til SATS, som opererer i flere land, burde etter Datatilsynets mening ha bedre rutiner og kontroll.
- De avdekte svakhetene og manglene påvirker rettighetene til så å si alle SATS-medlemmer (om lag 700 000), og ikke bare de fire medlemmene som hadde klaget til Datatilsynet.

SATS var raskt ute med å omtale gebyrets størrelse som en «betydelig overreaksjon». Hvorvidt gebyret blir stående gjenstår å se, men størrelsen viser at Datatilsynet både har evne og vilje til å utstede virkningsfulle og avskrekkende gebyrer. Etter DLA Pipers vurdering, illustrerer saken godt ringvirkningene av dårlige rutiner for rettighetshåndtering, som åpenbart får betydelig innvirkning på fastsettelsen av gebyret.

Det skal også bemerkes at Datatilsynet sendte avgjørelsen på sirkulasjon til tilsynsmyndighetene i Norge, Finland, Sverige og Danmark i henhold til «cross-border» regelen i GDPR artikkel 60, og at ingen av disse tilsynsmyndighetene hadde innvendinger mot verken vurderingene eller bøtenivået.

Tre viktige påminnelser

Etter DLA Piper sin vurdering, er denne avgjørelsen en viktig påminnelse til alle virksomheter som behandler personopplysninger om sine kunder. Etterlevelse av GDPR er ferskvare og krever en systematisk tilnærming i internkontrollen.

Våre tre ***«key takeaways»***, som alle virksomheter bør ta med seg i sine interne rutiner og praksis for behandling av personopplysninger, er som følger:

1. Vurder og dokumenter behandlingens formål og behandlingsgrunnlag *før* personopplysningene samles inn

Sørg for at virksomheten har angitt og dokumentert formålet med behandlingen av personopplysninger før personopplysningene samles inn. Formålsangivelsen danner utgangspunktet for virksomhetens plikter etter

GDPR og kan ikke senere justeres.

Behandlingsgrunnlaget skal også nøye vurderes, basert på formålet, før behandlingen iverksettes, og vurderingen skal dokumenteres. Etterfølgende vurdering reparerer *ikke* manglende dokumentasjon.

2. Personvernerklæringen må være korrekt, forståelig og lett tilgjengelig

Personvernerklæringen må tydelig få frem *hvorfor* personopplysninger behandles (formål), *grunnlaget for behandlingen* (behandlingsgrunnlag) og *hvor lenge de skal behandles* (lagringstid). Det er ikke tilstrekkelig å angi at personopplysninger behandles så lenge det er nødvendig, uten å presisere tidspunkt. Dersom det ikke er mulig å angi et konkret tidsperspektiv, må virksomheten angi kriteriene som brukes for å fastsette tidsrommet. Datatilsynet har kompetanse til å overprøve lagringstiden.

Personvernerklæringer er ferskvare og informasjonen som gis må stemme overens med virksomhetens rutiner og hvordan personopplysninger faktisk behandles. Videre må informasjonen som fremstilles være kortfattet og forståelig, fremstilt i et klart og enkelt språk. Det skal sette leseren i stand til å forstå hvilket behandlingsgrunnlag som benyttes for de enkelte behandlinger.

3. Rutiner skal ikke bare oppfylle lovkrav, de skal sikre etterlevelse og ansvarlighet i virksomheten

Interne rutiner for håndtering av forespørsler om innsyn, informasjon, sletting, etc., må være forståelig og lett tilgjengelige, slik at de blir kjent og brukt av ansatte som skal håndtere forespørslene.

Som et minimum må virksomheten utarbeide rutiner som sikrer at (1) henvendelsen blir vurdert, (2) at lovpålagt handling utføres, og (3) at avsender får et svar uten ugrunnet opphold og senest en måned etter mottak av henvendelsen.

I tillegg må rutinen tilpasses virksomheten – de må ha en struktur, et format og tilgjengelighet som sikrer at rutinene faktisk blir gjennomført av de ansatte.

DLA Piper har lang og bred erfaring med å bistå næringsdrivende med overholdelse av GDPR og personopplysningsloven. Ta gjerne kontakt med vårt team for Immaterialrett og Teknologi (IPT) ved spørsmål.

Fagområder	Immaterialrett og teknologi