Datatilsynet

WIKBORG REIN ADVOKATFIRMA AS
Postboks 1513 Vika

0117 OSLO

Gry Hvidsten

Deres referanse	Vår referanse	Dato
105879-564	20/03046-17	06/22.06.2022

Vedtak om overtredelsesgebyr - Trumf AS

1. Innledning

Vi viser til vårt varsel om vedtak om overtredelsesgebyr 6. desember 2021, samt svar på varselet fra Trumf 22. desember 2021.

2. Vedtak om pålegg og overtredelsesgebyr

Datatilsynet har i dag fattet følgende vedtak:

Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav i ilegges TRUMF AS org.nr. 976 912 047 et overtredelsesgebyr til statskassen på 5 000 000 kroner for:

- *Å ha brutt sine forpliktelser etter personvernforordningen artikkel 33 nr. 1 og artikkel 33 nr. 5*
- *Å ha brutt sine forpliktelser til å implementere egnede tiltak i henhold til personvernforordningen artikkel 32*

3. Nærmere om sakens faktiske forhold

Trumf AS («Trumf») er et fordelsprogram som tilbyr privatpersoner å spare bonus på kjøp i NorgesGruppens dagligvarebutikker og hos en rekke eksterne Trumf-partnere. Medlemmer i fordelsprogrammet kan registrere et bankkontonummer slik at det spares bonus på transaksjonene de utfører med bankkort som er knyttet bankkontoen. Trumf-medlemmet vil da få tilgang til detaljert informasjon om kjøp som er foretatt i butikkene tilknyttet Trumf, med visse unntak.[1] Informasjon om hvor man handlet, når man handlet, og hva man handlet vil være tilgjengelige for Trumf-medlemmet ved å logge inn på Trumf sine nettsider.

1 Apotek 1 anonymiserer noen av kjøpene som er foretatt hos dem.

Den 1. mars 2016 ble det gjennomført et møte mellom Trumf og Datatilsynet. Møtet ble initiert av Datatilsynet på bakgrunn av et tips til vår veiledningstjeneste i februar 2016. Dette tipset bestod i at en person hadde forsøkt å legge inn sitt eget kontonummer på sitt eget Trumf-medlemskap. Dette var imidlertid ikke mulig fordi en ukjent person allerede hadde registrert hans kontonummer. Vedkommende hadde ikke fått informasjon om at hans kontonummer var registrert hos Trumf.

På bakgrunn av innholdet i det mottatte tipset, samt møtet av 1. mars 2016, valgte Datatilsynet å initiere brevkontroll overfor Trumf for å undersøke om deres behandling av personopplysninger var i tråd med kravene i personopplysningsloven med forskrift.

Den 21. april 2016 skrev Trumf, blant annet, at de var klar over at medlemmer uriktig kan legge inn kontonummer til en tredjeperson. Trumf påpekte imidlertid at de hadde implementert løsninger med hensikt å hindre slik adferd; dersom et betalingskort tilknyttet en registrert bankkonto brukes står det «Trumf registrert» i displayet på betalingsterminalen, i tillegg til at fremgår av kvitteringen at Trumf-bonus er registrert i forbindelse med kjøpet. Trumf skrev for øvrig at å legge inn noen andre personer sine bankkontoopplysninger ville utgjøre et avtalebrudd.

Datatilsynet valgte 17. juli 2016 å varsle vedtak om pålegg mot Trumf, som bestod i:

- Pålegg om å sørge for rutiner for innhenting og kontroll av samtykke fra alle de behandler opplysninger om,

- Pålegg om å umiddelbart stanse behandling av kontonummer og andre personopplysninger som Trumf ikke har behandlingsgrunnlag for,

- Pålegg om å etablere rutiner for å sikre informasjon til de registrerte når Trumf samler inn eller på annen måte behandler opplysninger fra andre enn den som er medlem i Trumf,

- Pålegg om å utarbeide og tilstrekkelig dokumentere risikovurdering, akseptkriterier og tiltak som ledd i sitt informasjonssikkerhetsarbeid.

Disse påleggene var i stor grad tilknyttet det faktum at Trumf manglet en verifikasjonsløsning som sikret at Trumf-medlemmer kun registrerte sin egen bankkonto, og ikke andres. Herunder ga vi følgende bemerkning i varselet om vedtak:

> *Etter Datatilsynets oppfatning må Trumf sørge for en autentisering av knytningen mellom Trumf-medlemskap og kontoinnehaver, slik at det ikke er mulig å foreta behandling av kontonummer på trumf.no, med mindre kontoinnehaver og Trumf-medlem er samme person.*[2]

Den 15. august 2016 svarte Trumf på varselet om vedtak. I dette svaret fremgikk det, blant annet, at Trumf hadde vurdert ulike alternative måter for å verifisere at identiteten til bankkontoeier og medlemmet i Trumf er den samme, og funnet en metode for å sikre slik verifikasjon [redacted] Det fremgikk av svaret at det var noe usikkert når denne løsningen ville bli implementert, men etter opplysninger [redacted] skulle dette gjøres i løpet av høsten 2016. Trumf

2 Brev fra Datatilsynet, 17. juli 2016, «Varsel om vedtak – behandling av personopplysninger ved registering av kontonummer på trumf.no», side 7.

skrev at denne løsningen ville være hurtigere enn andre alternativer, og at dette var den beste måten å gjennomføre verifisering på.

Datatilsynet besluttet, i lys av Trumfs svar på varsel om vedtak, å avslutte saken. Datatilsynet bemerket i brev av 5. desember 2016, blant annet, at det var behov for en sterk autentisering (to-faktor) for at Trumf skal være trygg på at det er riktig person som samtykker til registering av kontonummer i Trumf. Datatilsynet bemerket at bruk av Bank-ID eller sikkerhetskode tilsendt på SMS virket som de beste forslagene for en sterk autentisering, blant annet fordi mobilnummer og fødselsnummer vil kunne verifiseres i [redacted] etter hvert som data blir lastet opp i denne databasen.

I 2020 ble Datatilsynet, gjennom media og ved kontakt med personvernombudet i Trumf, oppmerksom på at det fortsatt var mulig å legge inn andre personers bankkontonummer i Trumfs kundeprogram og at ingen verifikasjonsmekanisme hadde blitt implementert. På denne bakgrunn sendte Datatilsynet Trumf et krav om redegjørelse 2. oktober 2020.

I Trumfs redegjørelse av 9. november 2020 skriver de at siden 2016 har de jobbet målrettet med å adressere situasjonen, men at det har vært utfordrende å få realisert en tjeneste for verifikasjon av eierskap til bankkontoer. [redacted] Trumf skal ha løpende undersøkt andre muligheter for å få tilgang til en verifikasjonstjeneste.

Den 8. mars 2021 stilte Datatilsynet en rekke oppfølgingsspørsmål, blant annet ønsket vi en oppdatering på arbeidet med å finne en verifikasjonstjeneste, samt ytterligere innsikt i hvorfor Trumf ikke hadde sendt noen meldinger om brudd på personopplysningssikkerheten i tilfeller der Trumf hadde mottatt informasjon om feilregistreringer.

Den 20. april 2021 svarte Trumf at de ville få tilgang til en verifiseringstjeneste. Verifiseringsløsningen innebærer at medlemmet må identifisere seg med BankID. [redacted]

På spørsmålet om hvorfor hendelser av feilregistreringer ikke har blitt meldt til Datatilsynet svarte Trumf, blant annet, at den typiske situasjonen er at kontohaver ønsker å endre en registering som vedkommende allerede er kjent med. Videre viser Trumf til at det ofte er en tett relasjon mellom kontohaveren og Trumf-medlemmet, herunder familiemedlemmer eller andre økonomiske fellesskap. Trumf nevner videre at de ikke har mottatt henvendelser der det er mistanke om urettmessige registreringer med uærlige hensikter. De bemerker for øvrig at de i juni 2020 kontaktet tilsynet i forbindelse med spørsmålet om meldeplikt. Deres personvernombud skal i dialog med tilsynet ha gitt uttrykk for at Trumf ikke var av den oppfatning at det var tale om meldepliktige brudd på personopplysningssikkerheten, og sa hun var tilgjengelig dersom ytterligere dialog om emnet var nødvendig.

Ved innføringen av personvernforordningen i 2018 implementerte Trumf en digital løsning slik at medlemmene kunne be om innsyn og få tilgang til personopplysningene på trumf.no. Løsningen ble lansert for å oppfylle innsynretten medlemmene har etter regelverket.

Medlemmet kunne selv velge hvilke opplysninger, hvilket detaljnivå og hvilken periode det ønsket innsyn i ved å velge fra en liste over informasjonskategorier. Detaljert kjøpshistorikk var en av disse valgmulighetene. Det var kun tilgang til detaljer om medlemmet som var innlogget, slik at i et felles medlemskap vil medlemmene kun se detaljer om egne kjøp.

Trumf opplyser i e-post 30. november 2021 at brukerpanelet med den selvbetjente løsningen for innsyn ble betraktet som beste praksis på tidspunktet den ble innført. Trumf viser til at funksjonaliteten ble vist til Datatilsynet i et møte sommeren 2018, og at tilsynet ga en positiv tilbakemelding. Før den digitale løsningen ble lansert, ble innsynsretten håndtert av Trumf kundeservice.

I april 2020 ble detaljert kjøpshistorikk gjort tilgjengelig for medlemmene gjennom en egen knapp til digital «kvittering» fra kjøpshistorikken på trumf.no. Løsningen ble lansert slik at det skulle være enklere for medlemmene å verifisere bonusberegningen, ettersom det kan være ulike bonussatser på ulike varegrupper/varer. På den digitale kvitteringen kan medlemmet se varene per kjøp med tilhørende bonusberegning for den enkelte vare. Det er kun mulig å få tilgang til detaljene for det medlemmet som er innlogget, slik at i et felles medlemskap vil medlemmene kun se detaljer om egne kjøp.

I merknadene til varselet skriver Trumf at Datatilsynets vurdering tas til etterretning. Det framgår videre at Trumf ikke fullt ut er enig i Datatilsynets vurdering om brudd på personvernforordningen artikkel 32, men at det varslede gebyret aksepteres.

4. Regelverkets krav

4.1. Behandlingsansvarlig
Personvernforordningen artikkel 4 nr. 7 definerer «behandlingsansvarlig» som:

> […] *en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes; når formålet med og midlene for behandlingen er fastsatt i unionsretten eller i medlemsstatenes nasjonale rett, kan den behandlingsansvarlige, eller de særlige kriteriene for utpeking av vedkommende, fastsettes i unionsretten eller i medlemsstatenes nasjonale rett,*

4.2. Internkontroll og informasjonssikkerhet
De grunnleggende prinsippene for behandling av personopplysninger følger av personvernforordningen artikkel 5 nr. 1. I henhold til prinsippet om integritet og konfidensialitet, skal personopplysninger behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, jf. artikkel 5 nr. 1 bokstav f.

Dette innebærer blant annet at det må iverksettes egnede tekniske eller organisatoriske tiltak for å verne mot uautorisert eller ulovlig behandling, og mot utilsiktet tap, ødeleggelse eller endringer. Den behandlingsansvarlige skal kunne påvise at personvernprinsippene overholdes, jf. artikkel 5 nr. 2.

Som behandlingsansvarlig har man plikt til å gjennomføre egnede tekniske og organiske tiltak for å sikre og påvise at behandling av personopplysninger skjer samsvar med personvernforordningen, jf. artikkel 24. Det pliktes også å ha innebygd personvern og personvern som standardinnstilling i alle systemer og tjenester som behandler personopplysninger, jf. artikkel 25.

Kravene til personopplysningssikkerhet er nærmere regulert i artikkel 32. Den behandlingsansvarlige har plikt til å gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen. Avhengig av hva som er egnet, gjelder dette blant annet:

> a) pseudonymisering og kryptering av personopplysninger,
> b) evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og –tjenestene,
> c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,
> d) en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.

Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring, eller ikke-autorisert utlevering av eller tilgang til personopplysninger, jf. personvernforordningen artikkel 32 nr. 2.

4.3. Melding om brudd på personopplysningssikkerheten
Personvernforordningen artikkel 33 fastsetter at den behandlingsansvarlige i utgangspunktet plikter å melde «brudd på personopplysningssikkerheten» til Datatilsynet.

«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.

Det fremgår av artikkel 33 nr. 5 at «den behandlingsansvarlige skal dokumentere ethvert brudd på personopplysningssikkerheten […]. Denne dokumentasjonen skal gjøre det mulig for tilsynsmyndigheten å kontrollere samsvar med denne artikkel».

Skullerud m.fl. (ajourført versjon av kommentarutgaven til personvernforordningen, heretter omtalt som «kommentarutgaven») skriver følgende om denne forpliktelsen:

Uavhengig av om det foreligger meldeplikt til tilsynsmyndighetene eller ikke, så plikter den behandlingsansvarlige å dokumentere ethvert brudd på opplysningssikkerheten, herunder de faktiske forhold, potensielle konsekvenser og hvilke skadebegrensende tiltak som eventuelt ble iverksatt. Det må også dokumenteres hvilke vurderinger som ligger til grunn for at virksomheten eventuelt har unnlatt å melde fra om sikkerhetsbruddet til tilsynsmyndigheten

5. Datatilsynets vurdering

5.1. Behandlingsansvarlig
Det fremstår ikke omtvistet at det er Trumf som er behandlingsansvarlig, ettersom de bestemmer «formålet […] og hvilke midler som skal benyttes», jf. artikkel 4 nr. 7, i relasjon til behandlingsaktivitetene utført i konteksten av fordelsprogrammet Trumf.

5.2. Dagens løsning for å verifisere kundene
Datatilsynet legger til grunn at Trumf sin nåværende løsning, som beskrevet i brev 20. april 2021 og 3. juni 2021, sikrer at Trumf-medlemmer kun kan registrere bankkontoer som tilhører dem selv. Denne verifikasjonsløsningen innebærer at alle nye medlemmer må verifisere at de er innehaver av bankkontoen som de ønsker å registrere, før nytt medlemskap opprettes.

Eksisterende medlemmer vil måtte verifisere at de er innehaveren av bankkontoen de har registrert på Trumf når medlemmet logger på sin medlemskonto.

Dersom slik verifisering ikke gjennomføres vil vedkommende umiddelbart miste tilgang til funksjoner som innsyn i kjøpshistorikk og detaljerte kvitteringer. Medlemmet vil deretter gis en frist før kontoen slettes. Trumf jobber med å få verifisert alle kundene. I den anledning er det avholdt et møte mellom Datatilsynet og Trumf 20. juni 2022.

15. desember 2021 sendte Trumf inn en melding om brudd på personopplysningssikkerheten. Den nye tekniske løsningen medførte at innsyn i historiske transaksjoner og kvitteringer ble reaktivert, men dette inkluderte da eventuelle historiske transaksjoner fra betalingskort som var blitt avvist og ikke verifisert av kunden. Trumf fjernet muligheten for innsyn i historiske transaksjoner for medlemmer med avviste kontonummer, og beskriver videre i meldingen at det vil utvikles en løsning slik at medlemmer med avviste bankkontoer kun får innsyn i transaksjoner gjennomført med verifiserte bankkort, transaksjoner gjennomført etter at bankkontoen er verifisert, samt transaksjoner gjennomført med Trumf Visa og Trumf-kort. I møtet 20. juni forstod vi det slik at denne løsningen var på plass.

5.3. Brudd på personopplysningssikkerheten – artikkel 4. nr. 12
Det fremgår av artikkel 33 nr. 1 at ved «brudd på personopplysningssikkerheten» skal den behandlingsansvarlige, uten ugrunnet opphold og senest 72 timer etter å ha fått kjennskap til det, melde bruddet til tilsynsmyndighetene. Dette er imidlertid ikke nødvendig dersom bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter.

Meldeplikten vil kunne oppstå i tilfeller der sikkerhetsbruddet medfører en behandling som er ulovlig, men også dersom det medfører en behandling som er utilsiktet, uavhengig av hvorvidt behandlingen er ulovlig. Meldeplikten omfatter også hendelser som utgjør rene uhell.[3]

Trumf skriver i sin redegjørelse at de jevnlig har mottatt informasjon om tilfeller der Trumf-medlemmer registrerer andre personers bankkonto på deres eget Trumf-medlemskap.

Det første spørsmålet er hvorvidt det forekommer «brudd på personopplysningssikkerheten», jf. artikkel 33, jf. artikkel 4 nr. 12, når Trumf-medlemmer registrerer bankkontoer som ikke tilhører dem selv og på denne måten får tilgang til personopplysninger om handleturer utført av kontohaveren.

Trumf skriver i sin redegjørelse at de er av den oppfatning at dette ikke utgjør meldepliktige brudd på personopplysningssikkerheten, slik det er definert i personvernforordningen artikkel 4 nr. 12.

For det første henviser Trumf til at erfaringene fra henvendelsene til kundeservice er at de fleste berørte er klar over registreringen. For det andre at det typisk foreligger et økonomisk fellesskap, vanligvis et familie- eller bofellesskap, mellom Trumf-medlemmet og kontohaveren. For det tredje skal ingen ha tatt kontakt med kundeservice og angitt at tilgangen til kjøpshistorikk har vært opplevd som et problem.

Datatilsynet kan ikke se at disse innvendingene er relevante for om det er tale om et «brudd på personopplysningssikkerheten» etter artikkel 4 nr. 12.

Dersom et Trumf-medlem registrerer en annen person sin bankkonto vil Trumf behandle personopplysninger til kontohaveren, på utilsiktet vis. Trumf vil gjøre personopplysninger om vedkommende tilgjengelig for et Trumf-medlem, uten at dette er Trumfs intensjon. Trumf har selv vist til at registrering av andre sine bankkontoer utgjør avtalebrudd og i strid med retningslinjene for medlemskap i Trumf. En slik registering, og følgelig behandlingene av personopplysninger assosiert med dette, vil det derfor være et «brudd på sikkerheten som fører til utilsiktet […] tilgang til personopplysninger […]», jf. artikkel 4 nr. 12.

Trumf sine innvendinger fremstår mer relevante i vurderingen om hvor stor risiko bruddet på personopplysningssikkerheten vil kunne medføre for den registrerte (kontohaveren). En slik risikoavveining inngår imidlertid ikke i definisjonen av hva som utgjør et brudd på personopplysningssikkerhet, men er først relevant ved vurdering av om forholdet er meldepliktig etter artikkel 33 nr. 1. Se vår vurdering i punkt 5.5.

På denne bakgrunn har vi konkludert med at de tilfeller der et Trumf-medlem registrerer en annen person sin bankkonto på eget medlemskap så vil dette utgjøre et «brudd på personopplysningssikkerheten», jf. artikkel 4 nr. 12.

Trumf får, i henhold til sine egne anslag på bakgrunn av deres erfaringer fra 2021, informasjon om slike hendelser rundt 950 ganger i året.

3 Kommentarutgaven, i deres kommentarer til artikkel 33 nr. 1.

Datatilsynet har forståelse for at de 950 henvendelsene er estimert på bakgrunn av deler av 2021, og at det kan være noe usikkerhet knyttet til disse tallene. Trumf skriver imidlertid selv at de anser disse tallene til å være representative for tidligere år.[4] Videre er disse tallene estimert på bakgrunn av erfaringer innhentet etter at Trumf introduserte sitt nyeste informasjonstiltak, i form av at de tre første bokstavene til Trumf-medlemmet fremgår på kvitteringen etter et kjøp (dette tiltaket ble implementert i slutten av 2020). Det vil følgelig, i større utstrekning enn før, være mulig for kontohavere å direkte ta kontakt med Trumf-medlemmer som de kjenner igjen navnet til for å få fjernet registreringen. Dette vil kunne redusere antallet kontohavere som må ta kontakt med Trumf direkte for å få registreringen opphevet, sammenlignet med tidligere år. Selv om det ikke helt kan utelukkes, så er det iallfall ikke indikasjoner på at det er flere som tar kontakt i 2021 enn tidligere år.

Dersom vi legger til grunn erfaringene fra 2021 vil Trumf i gjennomsnitt få rundt 79 henvendelser om feilregistrering i måneden. For å illustrere omfanget så vil dette utgjøre over 3 000 henvendelser med informasjon om feilregistreringer i tidsperioden fra juni 2018 (da personopplysningsloven trådte i kraft) til oktober 2021. Dersom det istedenfor tas utgangspunkt i tidsperioden juni 2018 til juli 2020 (da personvernombudet tok kontakt med Datatilsynet for å blant annet meddele at de mener at disse hendelsene ikke er meldepliktige, og vi for øvrig fikk informasjon situasjonen gjennom media) har Trumf mottatt i underkant av 2 000 henvendelser om slike feilregistreringer.

Det er knyttet noe usikkerhet til de estimerte tallene, og eventuelt hvordan informasjonstiltaket på kvitteringen har påvirket dette. Ut fra det Trumf har redegjort for kan det uansett legges til grunn at Trumf har fått henvendelser i et betydelig omfang.

Hovedregelen er at alle brudd på personopplysningssikkerheten skal meldes til Datatilsynet. Det foreligger unntak fra meldeplikten dersom «bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter», jf. artikkel 33 nr. 1. Vi vurderer om hendelsene er unntatt fra meldeplikten i punkt 5.5, men først vurderer vi om Trumf har overholdt sin forpliktelse til å dokumentere bruddene på personopplysningssikkerhet i tråd med artikkel 33 nr. 5.

5.4. Artikkel 33 nr. 5

Trumf har informert om at kategorisering av ferdigbehandlende henvendelser ikke har blitt gjort før nylig. Trumf har kun presentert for Datatilsynet en grov kategorisering basert på en analyse av henvendelser behandlet i 2021.

Dersom det forutsettes at antallet henvendelser fra 2021 er representativ også for tidligere år, som lagt til grunn av Trumf, innebærer dette at Trumf har fått over 2 000 henvendelser om feilregistreringer av bankkontoer fra juni 2018 (da personopplysningsloven trådte i kraft) til slutten av 2020 (rundt da de begynte å kategorisere henvendelsene sine). Dette er kun et estimat, men tallene viser at det har vært en betydelig mengde slike henvendelser som ikke er kategorisert eller for øvrig dokumentert.

Trumf har følgelig ikke dokumentasjon som viser «[…] de faktiske forhold rundt nevnte brudd, virkningene av det og hvilke tiltak som er truffet for å utbedre det», jf. artikkel 33 nr. 5, for en rekke brudd på personopplysningssikkerheten.

4 Brev fra Wikborg Rein på vegne av Trumf, «Svar på nytt krav om redegjørelse – Behandling av personopplysninger ved registering av kontonummer via Trumf», 20. april 2021, side 2.

Denne dokumentasjonsforpliktelsen eksisterer uavhengig av om bruddet på personopplysningssikkerheten medfører risiko for fysiske personers rettigheter og friheter, og det er derfor ingen forutsetning at bruddet er meldepliktig etter artikkel 33 nr. 1.

På denne bakgrunn konkluderer Datatilsynet med at Trumf har brutt sin forpliktelse om å dokumentere bruddene på personopplysningssikkerheten som forekom fra 18. juni 2018 til utgangen av 2020, jf. artikkel 33 nr. 5.

Datatilsynet har imidlertid valgt å ikke problematisere om den overordnede kategoriseringen av hendelsene i 2021 oppfyller kravene i artikkel 33 nr. 5.

Det neste spørsmålet som Datatilsynet vil vurdere er om Trumf brøt sin forpliktelse etter artikkel 33 nr. 1 ved å ikke melde bruddene på personopplysningssikkerheten til Datatilsynet.

5.5. Artikkel 33 nr. 1

5.5.1. Risiko for fysiske personers rettigheter og friheter

Som konkludert ovenfor vil de tilfellene der et Trumf-medlem registrerer en annen person sin bankkonto på deres eget medlemskap utgjøre et «brudd på personopplysningssikkerheten», jf. artikkel 4 nr. 12.

Dersom bruddet på personopplysningssikkerheten «sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter», jf. artikkel 33 nr. 1, er det ikke nødvendig å melde det til Datatilsynet.

Det er den behandlingsansvarlige som må kunne underbygge at det ikke er risiko assosiert med bruddet på personopplysningssikkerheten. Dette fremkommer blant annet av fortalepunkt 85:

> *Så snart den behandlingsansvarlige får kjennskap til at det har oppstått et brudd på personopplysningssikkerheten, bør vedkommende melde nevnte brudd til tilsynsmyndigheten uten ugrunnet opphold og om mulig senest 72 timer etter å ha fått kjennskap til det, med mindre vedkommende i samsvar med ansvarlighetsprinsippet kan påvise at nevnte brudd på personopplysningssikkerheten sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter.* (egen utheving)

Det er følgelig Trumf som må vise til forhold som tilsier at bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Ordlyden i artikkel 33 nr. 1 tilsier også dette, ettersom det som skal sannsynliggjøres er at det *ikke* foreligger risiko.

Spørsmålet er dermed om Trumf kan underbygge at alle tilfellene omtalt ovenfor, der Trumf-medlemmer har registrert andre personer sin bankkonto på deres eget Trumf-medlemskap, «sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter», jf. artikkel 33 nr. 1.

I veilederen til Artikkel 29-gruppen om brudd på personopplysningssikkerhet, sist revidert februar 2018, fremgår det at det blant annet skal legges vekt på «the nature of the personal data».[5] Det skal tas i

5 Guidelines on Personal data breach notification under Regulation 2016/679, side 25.

betraktning om bruddet på personopplysningssikkerheten kan medføre skade eller øvrige negative konsekvenser. Dersom bruddet kan få konsekvenser for særlige sårbare individer må dette også inngå i vurderingen.[6]

Generelt er Datatilsynet av den oppfatning at bruddet på personopplysningssikkerheten i seg selv utgjør et inngrep i privatlivet til den som har fått registrert kontonummeret sitt hos Trumf uten viten og vilje. Handlehistorikken blir gjort tilgjengelig for uvedkommende og Trumf behandler personopplysninger om intetanende registrerte i større utstrekning enn tilsiktet. I tillegg til dette, eksisterer det et misbrukspotensiale. Sikkerhetshullet kan blant annet bli benyttet for å identifisere personer som bor på hemmelig adresse; dersom man har kontonummeret til en person som bor på hemmelig adresse, og registrerer dette på sitt Trumf-medlemskap, vil man få informasjon om hvor og når personen handler. Denne informasjonen kan gi klare indikasjoner på hvilke områder vedkommende oppholder seg i, eller for øvrig hvor vedkommende bor. At det kan ta så kort tid som [redacted] fra en person har handlet til et Trumf-medlem får informasjon om når, hvor og hva vedkommende har handlet, bidrar til å øke denne risikoen. Manglende verifisering av kontohavere kan derfor få konsekvenser for meget utsatte personer.

Det vil også kunne eksistere et betydelig misbrukspotensiale i tilfeller der kontohaveren og Trumf-medlemmet har en familiær eller økonomisk relasjon. Hva man handler kan avsløre private forhold. For eksempel kan handlemønsteret avdekke dietter og matvaner, kjøp av graviditetstester eller kjøp av prevensjonsmidler. Det kan heller ikke utelukkes at handlehistorikken til en person kan avsløre religiøse eller lignende forhold, for eksempel at man fraviker fra religiøse eller øvrige normer etablert i familien eller blant venner, eksempelvis ved å kjøpe alkohol eller visse typer kjøtt. Ved kjøp av, blant annet, glutenfrie produkter vil handlehistorikken også kunne avdekke kontohaverens allergier. [redacted]

[redacted]

At Trumf ikke har blitt direkte underrettet av kontohavere som har blitt eksponert for et slikt misbruk er ikke avgjørende. Trumf må ikke ha konkret og utvilsom kjennskap til at risikoen faktisk har materialisert seg. Dersom Trumf ikke klarer å vise at det «sannsynligvis ikke vil medføre en risiko […]», jf. artikkel 33 nr. 1, så skal bruddet på personopplysningssikkerheten meldes.

Trumf har imidlertid vist til en rekke generelle risikobegrensende tiltak som de har implementert. De ser ut til å være av den oppfatning at disse tiltakene medfører at en potensiell risiko assosiert med feilregistreringen blir eliminert, eller tilstrekkelig grad redusert. Ved bruk av et bankkort tilknyttet en registrert bankkonto så vil informasjon om Trumf-registeringen fremgå av bankterminalen og kvitteringen. I november 2020 la Trumf ytterligere informasjon på kvitteringen, ved at de tre første bokstavene i fornavnet til Trumf-medlemmet fremgår av kvitteringen.

6 Ibid.

7 Rutiner for risikovurdering side 4, vedlegg 5A til brev fra Wikborg Rein på vegne av Trumf, «Svar på krav om redegjørelse – behandling av personopplysninger ved registrering av kontonummer via Trumf», av 9. november 2020.

Datatilsynet er enig i at informasjonstiltak som er implementert av Trumf kan redusere tiden en kontoinnehaver forblir intetanende om registreringen. Imidlertid vil Trumf allerede ha behandlet personopplysninger om denne personen i større utstrekning enn hva de hadde gjort dersom bankkontoen ikke var registrert. Dette gjelder uavhengig av om det forutsettes at kontoinnehaveren umiddelbart får informasjonen om registreringen på sin første handletur etter å ha blitt registrert av et Trumf-medlem. Medlemmet som feilaktig registrerte bankkontoen til noen andre vil snarlig kunne ha fått informasjon om den registrertes handletur: som bemerket i redegjørelsen til Trumf vil det kunne ta så kort tid som [redacted] fra bankkortet er brukt til informasjon om handleturen blir tilgjengelig for medlemmet.

Det er for øvrig heller ikke gitt at kontohaveren vil bli gjort oppmerksom på registeringen gjennom informasjonstiltaket. At kundeservice får en rekke henvendelser etter at kontoinnehaveren har blitt oppmerksom på feilregistreringer, som følge av informasjonstiltakene, sier ikke noe om antallet kunder/kontohavere som *ikke* har oppdaget feilregistreringen gjennom disse informasjonstiltakene. Trumf vil aldri få informasjon om de kundene som ikke ser at det står «Trumf registrert» på betalingsskjermen, eller som for øvrig heller ikke prøver å registrere sin egen bankkonto på eget medlemskap.

I forlengelsen av dette, som Trumf selv bemerker i sin redegjørelse, forekommer det at kontohavere henvender seg til kundeservice fordi de selv forsøker å registrere sin egen bankkonto på eget medlemskap, men får da opplysning om at bankkontoen allerede er registrert (slike henvendelser estimerer Trumf til å være over 200 i året). Disse personene har følgelig ikke fått informasjon om registeringen via informasjonstiltakene beskrevet av Trumf. Dette er egnet til å illustrere hvordan personer vil kunne handle uten å legge merke til informasjonen. Samtidig kan det naturligvis ikke utelukkes at disse personene enda ikke hadde handlet i en butikk som var koblet til Trumf, etter at Trumf-medlemmet registrerte deres konto. Dette har for øvrig formodningen mot seg, ettersom det er et stort antall som hvert år tar kontakt etter å ha prøvd å registrere bankkontoen sin og deretter oppdaget at det allerede er registrert. Det fremstår usannsynlig at alle disse har prøvd å registrere seg på Trumf før sin første handletur.

Trumf har videre vist til hvordan det å registrere noen andre sitt kontonummer representerer et brudd på avtalevilkårene som Trumf-medlemmet inngår med Trumf, samt at det presiseres for medlemmet at de kun skal registrere kontoer som tilhører dem selv. Fra mai 2018 krevde registering av kontonummer også en to-faktor bekreftelse fra medlemmet, ved at en SMS-kode blir sendt til medlemmets registrerte mobiltelefonnummer.

Slike forhold kan redusere en mulig feilaktig antagelse hos Trumf-medlemmer om at det er akseptabelt å registrere andre personers bankkonto dersom det f.eks. er en familiær tilknytning mellom dem. Imidlertid har slike tiltak ingen reell innvirkning på de tilfeller der Trumf-medlemmet registrerer noen andre sin bankkonto bevisst i strid med avtalevilkårene, ettersom Trumf ikke har en verifikasjonsmekanisme. Disse tiltakene er heller ikke egnet til å forhindre ubevisste feilregistreringer, dersom medlemmet tror at de registrerer sitt eget kontonummer vil ikke slike tiltak være effektive. For øvrig illustrerer de stadige henvendelsene til kundeservice (estimert til å være 950 hvert år) at disse tiltakene ikke er tilstrekkelig for å fjerne risikoen for feilregistreringer.

Datatilsynet mener på denne bakgrunn at det er forhold ved ens handlehistorikk (herunder hva man handler, hvor man handler og når man handler) som tilsier at det vil eksistere en risiko tilknyttet tilfellene der en tredjepart får tilgang til slike personopplysninger, dette til tross for Trumf sine tiltak. Dette gjelder uavhengig av hvorvidt denne tredjeparten er et familiemedlem eller lignende.

Som et klart utgangspunkt mener Datatilsynet derfor at slike forhold skal meldes i henhold til artikkel 33 nr. 1, med unntak av de tilfellene der det kan vises til konkrete forhold ved bruddet som gjør at meldeplikten likevel ikke inntrer.

Trumf har, som bemerket ovenfor, konkludert med at ingen av henvendelsene de har mottatt, med beskjed om at det har forekommet feilregistreringer, har indikert tilstrekkelig grad av risiko for å aktualisere meldeplikten i artikkel 33. Trumf har kun gitt en overordnet beskrivelse av de ulike henvendelsene som de har mottatt, og plassert dem i ulike grupperinger basert på erfaringer fra starten av 2021. De bemerker i sin redegjørelse at vurderingen har en viss usikkerhet på grunn av varierende kvalitet og omfang av opplysninger fra dialogen med den som retter henvendelsen til kundeservice og Trumf-medlemmet som har kontoen registrert. Som kommentert ovenfor har ikke Trumf presentert noe dokumentasjon knyttet til bruddene på personopplysningssikkerheten som forekom før 2021, og de skriver at kategoriseringen av ferdigbehandlede henvendelser ikke har blitt gjort før nylig.

Datatilsynet vil gjennomgå disse typetilfellene i det følgende og kommentere eventuell risiko assosiert med dem, før det avslutningsvis konkluderes på hvilke brudd på personopplysningssikkerheten som Trumf kan sannsynliggjøre at det ikke foreligger risiko ved.

[redacted]

[redacted]

Konklusjon på risikovurderingen etter artikkel 33 nr. 1

Som bemerket ovenfor har Datatilsynet konkludert med at det eksisterer et misbrukspotensiale ved at Trumf-medlemmer kan registrere andre personer sitt kontonummer. Hvis Trumf får kjennskap til slike brudd på personopplysningssikkerheten skal disse i utgangspunktet meldes til Datatilsynet i samsvar med artikkel 33 nr. 1.

Dersom bruddene ikke meldes må Trumf kunne vise at de konkrete bruddene på personopplysningssikkerheten «sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter», jf. artikkel 33 nr. 1 og nr. 4.

Trumf har på et overordnet og generelt grunnlag vist til forhold ved de ulike henvendelsene som de mener medfører at det ikke er risiko for fysiske personers rettigheter og friheter. Beskrivelsen av de ulike typetilfellene er, som nevnt, generelle og de inneholder en rekke uklarheter.

Datatilsynet er for øvrig tilbakeholden med å overprøve en konkret risikoavveining, ettersom dette vil være en skjønnsmessig øvelse. Vi velger følgelig å forholde oss til de tilfellene der vi mener det er klart at Trumf ikke kan sannsynliggjøre at det ikke foreligger risiko for fysiske personers rettigheter og friheter. Dette gjelder de tilfellene der kontohaveren ikke var klar over at kontoen ble registrert på et Trumf-medlem, før vedkommende fikk informasjon om dette via, for eksempel, kvitteringen eller fordi personen har prøvd å registrere sin egen bankkonto på eget medlemskap.

I slike tilfeller vil kontohaveren ikke kunne foreta seg noe for å oppheve registeringen, ettersom personen – frem til vedkommende får slik informasjon – ikke vil ha noe kunnskap om registeringen. Kontohaveren vil for øvrig heller ikke kunne tilpasse hvor vedkommende handler, for å unngå at handlehistorikken blir gjort tilgjengelig for et en tredjepart. Trumf må kunne vise til klare konkrete holdepunkter som medfører at det allikevel sannsynligvis ikke foreligger risiko i slike tilfeller. Som gjennomgått ovenfor deler vi ikke Trumf sitt syn om at en familiær sammenheng eller et økonomisk fellesskap mellom Trumf-medlemmet og kontohaveren i seg selv sannsynliggjør at det ikke foreligger risiko for kontohaveren. Datatilsynet kan ikke utelukke at nærmere undersøkelser, i det konkrete tilfelle, kan avdekke at det allikevel ikke foreligger slik risiko, men Trumf har ikke gjennomført dette i relasjon til hvert enkelt brudd på personopplysningssikkerheten.

Datatilsynet konkluderer med at Trumf ikke har underbygget at brudd på personopplysningssikkerheten, i form av at Trumf-medlemmer registrerer andre personers bankkonto,

«sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter», jf. artikkel 33 nr. 1, i de tilfellene hvor kontohaveren ikke er kjent med registeringen fra begynnelsen av.

Spørsmålet blir dermed hvor mange brudd på personopplysningssikkerheten som har en slik karakter. Det fremgår følgende av Trumfs brev av 9. november 2020:

> *I følge kundeservice er det slik at størsteparten av dem som henvender seg dit og ber om bistand til å slette sitt kontonummer fra en annens medlemskap, selv har vært kjent med at kontoen har vært registrert på en annen person, typisk et nært familiemedlem. Den mest vanlige forklaringen som mottas fra personen som kontakter kundeservice er at vedkommende ønsker endring knyttet til samlivsbrudd eller liknende. Kun et lite mindretall av henvendelsene til kundeservice gjelder personer som sier de selv ikke har vært klar over registreringen. Dette gjelder færre enn 15 personer per måned – på årsbasis om lag 0,0001 % av medlemsmassen. Disse personene oppgir til kundeservice at de har fått kjennskap til registreringen, når de har forsøkt å registrere seg som nytt medlem, eller når de har sett av kvitteringen at det er en Trumf-registrering på kontoen som de ikke kjenner til. Dette viser nettopp at informasjonstiltakene fungerer.* [vår utheving].

[redacted]

Det er ikke nødvendig for Datatilsynet å ta stilling til det nøyaktige antallet brudd på personopplysningssikkerheten som Trumf ikke kan sannsynliggjøre ikke utgjør en risiko for fysiske personers rettigheter og friheter. Det er tilstrekkelig å konstatere at Trumf har jevnlig, minst 15 ganger i en gjennomsnittlig måned, mottatt slike henvendelser.

5.5.2. Kjennskap til bruddet på personopplysningssikkerheten

I vurderingen har vi kun tatt utgangspunkt i de henvendelsene som Trumf har mottatt informasjon om gjennom sin kundeservice. Det er følgelig ikke tvilsomt at Trumf gjentatte ganger har oversittet 72-timersfristen, som fremgår av artikkel 33 nr. 1.

5.5.3. Konklusjon om brudd på personopplysningssikkerhet

Datatilsynet har påvist hvordan tilfeller der et Trumf-medlem registrerer andre sine kontonumre utgjør et «brudd på personopplysningssikkerheten», jf. artikkel 4 nr. 12.

Utgangspunktet er at tilsynsmyndighetene skal meldes om brudd på personopplysningssikkerheten i henhold til artikkel 33 nr. 1. Datatilsynet har konkludert med at Trumf, i en rekke tilfeller, ikke kan sannsynliggjøre at det ikke foreligger risiko for fysiske personers rettigheter og friheter, jf. artikkel 33 nr. 1. Meldingens innhold må utformes i overenstemmelse med artikkel 33 nr. 3.

Datatilsynet har ikke mottatt noen meldinger om brudd på personopplysningssikkerheten fra Trumf. Vi konkluderer derfor med at Trumf gjentatte ganger har brutt sin forpliktelse etter artikkel 33 nr. 1, om å sende Datatilsynet meldinger om brudd på personopplysningssikkerheten.

Vår konklusjon innebærer ikke at Trumf måtte ha sendt én melding for hver enkelt hendelse. Artikkel 29-gruppen beskriver muligheten for å gi samlede meldinger i tilfeller der det forekommer gjentatte brudd på personopplysningssikkerheten med lignende innhold og fremgangsmåte:

> *Strictly speaking, each individual breach is a reportable incident. However, to avoid being overly burdensome, the controller may be able to submit a "bundled" notification representing all these breaches, provided that they concern the same type of personal data breached in the same way, over a relatively short space of time. If a series of breaches take place that concern different types of personal data, breached in different ways, then notification should proceed in the normal way, with each breach being reported in accordance with Article 33.*[8]

5.6. Sikkerhet ved behandlingen - artikkel 32

Artikkel 32 etablerer en plikt for Trumf til å gjennomføre egnede tekniske og organisatoriske tiltak for å sørge for et sikkerhetsnivå som er egnet med hensyn til risikoen. Hva som utgjør egnende tekniske og organisatoriske tiltak beror på «[…] 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 […]».

Trumf bestrider ikke sine forpliktelser etter artikkel 32, men skriver at restrisikoen for individenes rettigheter og friheter er på et akseptabelt nivå i lys av deres allerede gjennomførte tiltak.

Spørsmålet som Datatilsynet skal ta stilling til er om Trumf har implementert «egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen […]», jf. artikkel 32 nr. 1. Vi vil ta utgangspunkt i sikkerhetsnivået som eksisterte før verifikasjonsløsningen ble implementert.

Trumf har over lengre tid jevnlig mottatt henvendelser om at feilregistreringer forekommer, i form av at Trumf-medlemmer registrerer andre personer sine bankkontoer på eget medlemskap. Dette medfører at Trumf får klar informasjon om stadige tilfeller av «ikke-autorisert utlevering av eller tilgang til personopplysninger […]», jf. artikkel 32 nr. 2 og brudd på «[…] konfidensialitet […] i behandlingssystemene og tjenestene» sine, jf. artikkel 32 nr. 1 bokstav b.

Som vi omtalte ovenfor vil det kunne eksistere en klar risiko for fysiske personers rettigheter og friheter ved at en tredjepart får tilgang til personopplysninger om handlehistorikk (herunder handlested, hva man har handlet og når man har handlet). Dette vil kunne avdekke inngående private forhold, og

8 Guidelines on Personal data breach notification under Regulation 2016/679, side 16.

vil uansett kunne oppleves ubehagelig. Denne risikoen er enhver, som ikke allerede har registrert kontonummeret sitt i Trumf, eksponert for.

Denne risikovurderingen må ta i betraktning sannsynligheten for mulige hendelser som kan ha forekommet uten at Trumf har fått konkret kjennskap til dem, samt mulige fremtidige konsekvenser. Trumf kan i denne anledning ikke anføre manglende konkret kunnskap om, for eksempel, at personer på hemmelig adresse har blitt avslørt, eller at tredjeparter har brukt informasjonen tilgjengelig for dem for å avdekke om kontohaverne er hjemme eller for eksempel på ferie.

Trumf har truffet visse risikobegrensende tiltak, blant annet at det står «Trumf registrert» i betalingsdisplayet samt at det fremgår informasjon om Trumf-medlemskapet på kvitteringen. I senere tid har Trumf supplert med ytterligere informasjon på kvitteringen, i form av at de tre første bokstavene til Trumf-medlemmet fremgår. Det er videre nødvendig å bruke mobiltelefonen sin for å registrere en bankkonto.

Datatilsynet mener at disse tiltakene ikke er tilstrekkelig for å oppnå et sikkerhetsnivå som er påkrevd etter artikkel 32.

Som nevnt ovenfor viser de gjentatte henvendelsene der kontohaveren først får informasjon om registeringen på tidspunktet da kontohaveren selv forsøker å registrere kontoen sin på eget medlemskap, at informasjonstiltakene ikke er tilstrekkelig effektive. Videre, selv dersom kontohaveren får informasjon om registeringen etter en stund via slike informasjonstiltak vil en potensiell skade allerede kunne ha forekommet.

Trumf har gitt deres medlemmer tilgang til informasjon om handlested og handlehistorikk, til tross for at Trumf har manglet en verifikasjonsløsning. Videre har Trumf hatt konkret kjennskap til at det stadig ble gjennomført feilregistreringer, i strid med medlemsvilkårene sine. Dette skaper en klar oppfordring til å reagere.

Denne risikoen ville kunne ha blitt redusert betydelig gjennom tekniske og organisatoriske tiltak.

Dersom Trumf hadde fjernet eller betydelig redusert informasjonen om handlested, handletid og hva som ble handlet, ville ikke kontohaverne lenger være utsatt for den aktuelle risikoen. Gjennomføringskostnadene assosiert med å begrense mengden opplysninger som er tilgjengelig for et Trumf-medlem vil trolig være begrenset.

Datatilsynet har forståelse for at slik informasjon kan være populær blant Trumf-medlemmene, og at å begrense slik informasjon (oversikt over handletidspunkt, handlested og hva som ble kjøpt) vil redusere innsynet i detaljer om grunnlaget for bonusopptjening. Imidlertid vil fortsatt Trumf-løsningen fungere i tråd med sitt primære formål. Trumf bemerket selv i sitt brev 21. april 2016, at Trumf er et lojalitetsprogram der medlemmer får beregnet bonus etter kjøpshistorikk, og formålet med å registrere bankkontonummer er å forenkle innsamlingen av bonusgrunnlag. Dette formålet vil fortsatt kunne forfølges, selv ved tiltak som betydelig begrenser informasjonsmengden som er tilgjengelig for Trumf-medlemmet, så lenge Trumf ikke kan verifisere at medlemmet har registrert sin egen konto.

Trumf har tidligere uttrykt at de mener at informasjonen om handlehistorikken som blir gjort

tilgjengelig for Trumf-medlemmet sikrer en personvernvennlig løsning, ved at brukeren har enkel tilgang til sine egne personopplysninger. Trumf ser følgelig ut til å være av den oppfatning at et tiltak, i form av å redusere opplysninger om handlehistorikk, ikke er egnet å implementere som følge av slike ulemper.

Datatilsynet er ikke enig i at dette er en personvernvennlig løsning, i lys av sakens omstendigheter. Det fremgår av artikkel 12 nr. 2 forutsetningsvis at den behandlingsansvarlige ikke er forpliktet til å legge til rette for at den registrerte kan utøve sine rettigheter etter artikkel 15 til 22 dersom den behandlingsansvarlige ikke er i stand til å identifisere den registrerte. Løsningen til Trumf, i lys av at de ikke har klart å verifisere at medlemmet registrerer sin egen konto, er følgelig ikke en personvernvennlig løsning, men utgjør en risiko for fysiske personers rettigheter og friheter.

For øvrig må «behandlingens […] omfang» tas i betraktning i vurderingen av egnede tekniske og organisatoriske tiltak. Trumf sitt lojalitetsprogram har rundt 2,395 millioner medlemmer, hvorav [redacted] har registrert bankkonto. Tallene tilsier at i overkant av [redacted] personer har registrert bankkontoer i løsningen, uten at Trumf vet om kontonumrene tilhører Trumf-medlemmene de er registrert på.

Trumf opplyser for øvrig hvordan de har «løpende fulgt opp andre muligheter for tilgang til en verifikasjonstjeneste».[9] [redacted] Imidlertid, som vi har påpekt ovenfor, viser erfaringene fra Trumf sin kundeservice at dette ikke forhindret feilregistreringer.

[redacted]

Datatilsynet mener at det finnes klart egnede tiltak som ville betydelig redusert akkurat de risikoene som Trumf selv identifiserer. Trumf er selv oppmerksom på lignende tiltak, ettersom de i 2016 omtalte muligheten for å redusere mengden informasjon som var tilgjengelig for Trumf-medlemmene.

Trumf skriver i merknadene at de ikke er enig i Datatilsynets vurderinger av brudd på personvernforordningen artikkel 32 ettersom en del av tiltakene ble implementert da det ikke var tilgjengelig noen verifikasjonsløsing i markedet. Datatilsynet er derimot av den oppfatning at da det ble klart at Trumf ikke snarlig kunne iverksette en verifikasjonsløsning skulle Trumf ha redusert risikoen

9 Brev fra Wikborg Rein, på vegne av Trumf, «Svar på krav om redegjørelse – behandling av personopplysninger ved registering av kontonummer via Trumf», 9. november 2020.

for at Trumf-medlemmer kunne få tilgang til andres personopplysninger, for eksempel ved å fjerne, eller betydelig redusere, informasjonen om handlested, tid og informasjon om hva som ble handlet for medlemmene, frem til de fikk klarhet i at de ikke utleverte personopplysninger om kontohaveren til andre.

I lys av det ovenstående konkluderer vi med at Trumf ikke har implementert «egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen […]», jf. artikkel 32 nr. 1.

Datatilsynet konkluderer med at Trumf brøt sin forpliktelse etter artikkel 32.

I 2016 bemerket, som nevnt, Trumf muligheten for å implementere ett risikoreduserende tiltak, i påvente av at de kunne sikre tilstrekkelig grad av verifikasjon. Trumf ba om veiledning på dette punktet.

> [F]*or å avhjelpe risiko for at kjøpshistorikk kan brukes til å finne ut hvor tredjepersoner faktisk har oppholdt seg vil Trumf, inntil forholdet kontoeier - kontonummer er verifisert, kunne skjule stedsnavnet til butikken i handlehistorikken, som beskrevet i punkt 3 nedenfor. Denne løsningen er ferdig og kan iverksettes umiddelbart. Løsningen vil imidlertid innebære redusert innsyn for det store flertallet av medlemmer, som da mister et innebygget personverntiltak på trumf.no. Trumf ber om Datatilsynets veiledning på om tiltaket bør iverksettes.*[10]

Datatilsynet besvarte imidlertid ikke denne forespørselen om veiledning i 2016.

At Trumf søkte veiledning, og følgelig vurderte muligheten for et konkret risikobegrensende tiltak, får en viss betydning i vurderingen av alvorlighetsgraden av bruddet. Dette adresserer vi ytterligere under punkt 6.2.

For øvrig er ansvaret etter artikkel 32 plassert hos den behandlingsansvarlige, noe som også følger av ansvarlighetsprinsippet, jf. artikkel 5 nr. 2. Dette poenget blir også understreket i kommentarutgaven. At det ble søkt veiledning hos Datatilsynet endrer derfor ikke standpunktet om at Trumf har brutt sin forpliktelse etter artikkel 32. Dette er særlig tilfellet i lys av at nytt regelverk har blitt implementert i mellomtiden, som må anses til å særlig aktualisere en ny, selvstendig, vurdering fra Trumf sin side.

Videre må det bemerkes at Trumf også hadde visse informasjonstiltak iverksatt i 2016. Datatilsynet var også da, som fremgår helt tydelig for Trumf i varselet om vedtaket av 17. juni 2016, av den oppfatning at slike informasjonstiltak ikke i tilstrekkelig grad reduserte risikoen for feilregistreringer og at en verifikasjonsløsning var nødvendig for å sørge for tilstrekkelig informasjonssikkerhet. Da verifikasjonsløsningen allikevel ikke ble tilgjengelig hadde Trumf en klar oppfordring til å undersøke alternative risikoreduserende tiltak. Manglende veiledning fra Datatilsynet på dette punktet må ses i lys av at tilsynet var av den oppfatning at Trumf ville sikre en verifikasjonsløsning snarlig.

Som nevnt ovenfor har vi konkludert med at Trumf har brutt artikkel 32, men vi ilegger ikke Trumf

10 Brev fra Wikborg Rein på vegne av Trumf, «Svar å varsel om vedtak – Registering av kontonummer på Trumf.no», 15. august 2016.

pålegg om å implementere slike organisatoriske og/eller tekniske tiltak, ettersom Trumf nå har implementert en verifikasjonsløsning.

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, og varsler med dette ileggelse av overtredelsesgebyr, jf. personvernforordningen artikkel 83. I samsvar med Høyesteretts praksis (jf. Rt. 2012 side 1556) legger vi til grunn at overtredelsesgebyr er å anse som straff etter den europeiske menneskerettighetskonvensjonen artikkel 6. Det kreves derfor klar sannsynlighetsovervekt for lovbrudd for å kunne ilegge gebyr.

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

6.2. Vurdering av om overtredelsesgebyr skal ilegges

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

Vi vil her vurdere de relevante momentene fortløpende.

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

Datatilsynet er av den oppfatning at alvorlighetsgraden taler for ileggelse av overtredelsesgebyr. Trumf har i dag rundt 2,4 millioner medlemmer. Alle medlemmene har hatt mulighet til å registrere kontonumre på sine medlemskap, uten at Trumf har verifisert at kontonumrene tilhører medlemmene de er knyttet til. Denne svakheten har vært åpen i Trumf sine systemer i mange år. Trumf har ikke bare vært kjent med at det er risiko for feilregistreringer i løsningen deres, men har også hatt konkret kunnskap om at denne risikoen stadig materialiserer seg.

Sakens bakgrunn skjerper alvorlighetsgraden. I 2016 gjorde Datatilsynet det klart at vi så alvorlig på situasjonen, og understrekte overfor Trumf hvor sentralt det var å sikre verifikasjon, ettersom vi var av den oppfatning at manglende verifikasjon åpnet opp for misbruk av løsningen. Dette medførte at Datatilsynet varslet et vedtak rettet mot Trumf, som blant annet innebar at de måtte stanse behandling av kontonummer og andre personopplysninger som Trumf ikke hadde behandlingsgrunnlag for (Datatilsynet mente at Trumf manglet behandlingsgrunnlag i tilfeller der Trumf-medlemmet registrerte noen andre sin kontonummer, i lys av manglende verifikasjonsmekanisme).

Datatilsynet valgte likevel ikke å treffe endelig vedtak i saken ettersom Trumf ga utfyllende informasjon om hvordan de, blant annet, snarlig skulle ta i bruk en løsning [redacted] som ville

sikre at Trumf-medlemmer kun hadde mulighet for å registrere egne bankkontonumre. Trumf ble imidlertid allerede i vinteren 2016/2017 klar over at det ikke var mulig å bruke [redacted]. At Trumf brøt sin meldeplikt under slike forhold må karakteriseres som alvorlig.

Omfanget av overtredelser av artikkel 33 nr. 1 er utfordrende for Datatilsynet å fastslå. Basert på estimatene gitt av Trumf har de fått et betydelig antall henvendelser om feilregistreringer, som Datatilsynet mener Trumf skulle ha meldt i tråd med artikkel 33 nr. 1. Samtidig er Datatilsynet varsom med å legge for stor vekt på det store antallet av brudd på personopplysningssikkerheten, ettersom det eksisterer noe usikkerhet rundt tallene. Vi er særlig tilbakeholden med å vektlegge manglende meldinger knyttet til bruddene på personopplysningssikkerheten som Trumf mottok etter juni 2020. På dette tidspunktet kontaktet Trumfs personvernombud Datatilsynet, og gav informasjon om at de ikke vurderte tilfeller av feilregistreringer som meldepliktige brudd.

Det sentrale for Datatilsynet er at Trumf har hatt gjentatte brudd på personopplysningssikkerheten som ikke har blitt meldt til Datatilsynet, til tross for at Trumf var kjent med Datatilsynet sin oppfatning om at manglende verifisering av kontonumre medfører en risiko for kontohaverne sine rettigheter og friheter.

Vedrørende artikkel 33 nr. 5 er det sentralt at virksomheter dokumenterer sine brudd på personopplysningssikkerheten. Slik dokumentasjon er ikke kun ment til å sørge for at Datatilsynet kan vurdere om den behandlingsansvarlige overholder sine forpliktelser i relasjon til artikkel 33, men vil også være nyttig for den behandlingsansvarliges arbeid med å sørge for tilstrekkelig grad av sikkerhet.[11] At Trumf ikke har sørget for slik dokumentasjon er i seg selv et brudd, samtidig som det har gjort det vanskeligere for Datatilsynet å undersøke Trumf sin etterlevelse av artikkel 33 nr. 1.

Datatilsynet har forståelse for at vurderingen som gjøres etter artikkel 33 nr. 1, rundt risikoen for de registrertes rettigheter og friheter, er skjønnsmessig og at denne kan være utfordrende i det konkrete tilfellet. Plikten til å dokumentere brudd etter artikkel 33 nr. 5 er imidlertid klar og mangler skjønnsmessige vurderinger.

Trumf har fremsatt noen argumenter om hvorfor de mener at tilfeller av feilregistrering ikke representerer et «brudd på personopplysningssikkerheten», som vi gjennomgikk ovenfor. Disse var i realiteten kun relevante ved risikovurderingen etter artikkel 33 nr. 1, og fremstod ikke som relevante for vurderingen av om slike feilregistreringer i seg selv oppfyller definisjonen i artikkel 4 nr. 12. Det fremstår for Datatilsynet klart at slike hendelser er «brudd på personopplysningssikkerheten».

Bruddet på artikkel 33 nr. 5 må videre ses i lys av kommunikasjonen mellom Trumf og Datatilsynet i 2016, da det ble klart for Trumf at de ikke ville klare å implementere en verifikasjonsløsning, som først beskrevet for Datatilsynet. At dokumentasjon og gruppering av feilregistreringene først, tilsynelatende, ble iverksatt i 2021 anser vi, under disse omstendighetene, som alvorlig. Datatilsynet har for øvrig valgt å ikke problematisere om de overordnede beskrivelsene og grupperingene gitt av 2021-tilfellene er tilstrekkelige for å oppfylle artikkel 33 nr. 5.

Som bemerket har Datatilsynet også konkludert med at Trumf brøt sin forpliktelse etter artikkel 32, som følge av at Trumf ikke implementerte egnede tiltak da de ble oppmerksomme på at en

11 Kommentarutgaven i relasjon til artikkel 33 nr. 5.

verifikasjonsløsning ikke kunne implementeres på kort sikt. Imidlertid beskrev Trumf muligheten for å begrense noe av informasjonsmengden som ble tilgjengelig for Trumf-medlemmene tilbake i 2016. Trumf forespurte Datatilsynet om veiledning angående tiltaket, men Datatilsynet besvarte ikke denne forespørselen. Vi tar hensyn til dette i vår vurdering av alvorlighetsgraden. Samtidig må vi understreke at ansvaret etter artikkel 32 er plassert hos den behandlingsansvarlige, og Trumf hadde enhver foranledning til å gjennomføre en ny selvstendig vurdering, særlig i lys av at nytt personvernregelverk trådte i kraft etter at de søkte veiledning fra Datatilsynet. Videre hadde ikke Datatilsynet en sterk oppfordring til å gi slik veiledning eller uttale seg om emnet ettersom Trumf gav informasjon om at de ville implementere en verifikasjonsløsning snarlig.

I tillegg må det fremheves, som ovenfor, at Datatilsynet i 2016 varslet at Trumf måtte utarbeide og tilstrekkelig dokumentere risikovurdering, akseptkriterier og tiltak som ledd i sitt informasjonssikkerhetsarbeid. Datatilsynet skrev følgende om dette punktet, under overskriften «Informasjonssikkerhet og internkontroll»:

> *Slik situasjonen er i dag medfører løsningen på trumf.no at det enkelt kan skje uautorisert behandling av kontonummer, stedsdata og handlehistorikk for husstandsmedlemmer og personer som ikke medlem i Trumf. Etter Datatilsynets oppfatning må Trumf sørge for en autentisering av knytningen mellom Trumf-medlemskap og kontoinnehaver, slik at det ikke er mulig å foreta behandling av kontonummer på trumf.no, med mindre kontoinnehaver og Trumf-medlem er samme person. Kunnskap om hvem som er kontoinnehaver er i tillegg en forutsetning for å innhente og kontrollere at det foreligger gyldig samtykke fra den registrerte.*

Denne uttalelsen synliggjorde for Trumf hvordan sikkerhetsnivået, som følge av manglende verifikasjonsløsning, ikke var tilstrekkelig. Ytterligere tiltak var nødvendig, i tillegg til at Datatilsynet mente at behandlingsgrunnlag måtte sikres. Som tidligere bemerket var årsaken til at Datatilsynet ikke fulgte opp dette varselet, blant annet, at Trumf skrev at de ville sikre en verifikasjonsløsning. At egnede tiltak, som identifisert ovenfor, ikke ble iverksatt da det ble klart at Trumf allikevel ikke ville kunne få implementert en verifikasjonsløsning må anses kritikkverdig.

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

At Trumf-medlemmer registrerer andres kontonummer på sitt medlemskap er ikke forsettlig av Trumf, tvert imot er en slik registering i strid med Trumf sine avtalevilkår. Imidlertid er det klart at det har vært forsettlig av Trumf å ikke melde fra om disse hendelsene til Datatilsynet. Trumf tok også et bevisst valg om å ikke implementere tiltak som reduserte risikoen for misbruk som eksisterte på grunn av manglende verifikasjonsmekanisme. Overtredelsene i relasjon til artikkel 33 nr. 1 og 32 anser vi følgelig å være forsettlige, ved virksomhetens ledelse. Dette trekker i skjerpende retning.

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

I Artikkel 29-gruppens retningslinjer om overtredelsesgebyr 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]

Artikkel 29-gruppen 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.*

Trumf har implementert informasjonstiltak som er ment å gjøre kontohavere oppmerksom på om deres bankkonto er registrert på et Trumf-medlemskap, og følgelig øke sjansen for å avdekke feilregistrering. Videre innførte de i 2018 to-faktorautentisering gjennom SMS til medlemmets registrerte telefonnummer. At Trumf har truffet slike tiltak er et argument mot overtredelsesgebyr. Trumf iverksatte imidlertid ikke tiltak for å redusere informasjonen tilgjengelig for medlemmene deres, i tilfelle det skulle forekomme feilregistreringer – som Trumf visste forekom mange ganger i året. Slik informasjonsbegrensning ville kunne redusert skaden for de registrerte. I likhet med hva som ble kommentert ovenfor tar vi i betraktning det faktum at Trumf søkte veiledning fra Datatilsynet om tiltak som skulle implementeres.

> *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*

Trumf har brutt sin forpliktelse etter artikkel 32, som følge av manglende egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet i lys av risikoen. Dette taler derfor for ileggelse av overtredelsesgebyr.

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

Vi har ikke identifisert noen tidligere relevante overtredelser, og dette forholdet taler dermed ikke for ileggelse av overtredelsesgebyr.

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

Trumf har samarbeidet med Datatilsynet, og besvart de spørsmålene som ble stilt. Dette er imidlertid Trumf pålagt å gjøre. Artikkel 29-gruppen bemerker i denne anledning følgende:

> […] *it would not be appropriate to give additional regard to cooperation that is already required by law for example, the entity is in any case required to allow the supervisory authority access to premises for audits/inspections.*

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

At Trumf har gitt utfyllende svar på Datatilsynets krav på redegjørelser er ikke en formildende omstendighet i seg selv.

Imidlertid tok Trumfs personvernombud, i forbindelse med oppslagene i media, kontakt med Datatilsynet for å forhøre seg om tilsynets videre prosess, samt for å informere overordnet om de tiltak Trumf hadde iverksatt. Dette trekker i en noe formildende retning, isolert sett.

For øvrig ble det allerede i vinteren 2016/2017 klart at Trumf ikke ville kunne implementere verifikasjonsløsningen som Trumf forespeilet Datatilsynet da vi avsluttet saken i 2016. Trumf gav ikke tilsynet noe informasjon om dette. Dersom Datatilsynet hadde fått informasjon om at utfordringen med verifikasjon ikke allikevel ville bli løst kunne vi ha vurdert muligheten for å, for eksempel, pålegge Trumf å begrense mengden personopplysninger som ble tilgjengelig for Trumf-medlemmet. Trumf var pålagt å gi oss slik informasjon, i lys av at manglende verifikasjonsmekanisme ledet til gjentatte tilfeller av meldepliktige brudd på personopplysningssikkerheten. Graden av samarbeid med tilsynsmyndighetene har på dette grunnlag ikke blitt ansett som en formildende omstendighet av særlig betydning.

g) kategoriene av personopplysninger som er berørt av overtredelsen

Artikkel 29-gruppens veileder viser til at vurderingen under bokstav g blant annet knytter seg til om spredning av personopplysninger kan medføre skade eller ubehageligheter for de registrerte.[13] Vi viser til tidligere kommentarer rundt misbrukspotensialet som eksisterer som følge av at Trumf-medlemmer kan få opplysninger om kjøpshistorikk mv. til andre personer.

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

Datatilsynet fikk i 2020, via omtale i media og kontakt med personvernombudet, vite om at verifikasjonsløsningen ikke var implementert i tråd med Trumf sin fremdriftsplan fra 2016. På tidspunktet da personvernombudet tok kontakt med Datatilsynet var det nærliggende at media ville ytterligere beskrive hvordan Trumf ikke hadde implementert en verifikasjonsløsning. Til tross for dette må kontakten fra personvernombudet vektlegges som en formildende omstendighet under bokstav h.

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

Datatilsynet varslet i 2016 vedtak om pålegg mot Trumf. Dette resulterte imidlertid ikke i et endelig vedtak, og relaterte seg til gammelt regelverk. Vi benyttet av denne årsak aldri kompetansen som fremgår av artikkel 58 nr. 2. Dette forholdet er derfor ikke relevant ved vurdering av om overtredelsesgebyr skal ilegges.

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

13 Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, side 14.

Vi finner ikke dette momentet relevant.

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

Personvernnemnda har i sin praksis slått fast at lang saksbehandlingstid skal utgjøre en formildende omstendighet. I PVN-2021-03 legger Personvernnemnda vekt på at sakens faktum ble i det vesentlige avklart i mai 2019, mens det tok over ett år før tilsynet varslet pålegg og overtredelsesgebyr. I PVN-2021-09 la Personvernnemnda også vekt på den lange saksbehandlingstiden hos tilsynet. I den saken hadde det gått seks måneder fra tilsynet mottok en melding om brudd på personopplysningssikkerhet til det ble bedt om en redegjørelse. Etter å ha mottatt redegjørelsen tok det ca. fire måneder før varsel om vedtak ble sendt, og deretter ti måneder fra varselet ble sendt til vedtaket ble fattet. Etter at virksomheten klagde gikk det ytterligere tre måneder før saken ble mottatt av Personvernnemnda. Høyesterett har for øvrig i sin praksis lagt til grunn at først ved total inaktivitet på rundt ett år anses saksbehandlingstiden til å bryte med den europeiske menneskerettighetskonvensjonen.[14]

Denne saken ble igangsatt ved at Datatilsynet sendte Trumf et krav om redegjørelse. Dette kravet om redegjørelse ble sendt 2. oktober 2020. Trumf, ved deres representant, ba om forlenget frist for å besvare Datatilsynets spørsmål. Denne forespørselen ble innvilget. Datatilsynet mottok redegjørelsen til Trumf 9. november 2020. Nytt krav om redegjørelse ble sendt Trumf den 8. mars 2021. Den 23. mars 2021 fikk Trumf innvilget utsatt frist for å svare på redegjørelsen. Den 20. april 2021 mottok Datatilsynet Trumfs nye redegjørelse. Den 3. juni 2021 fikk Datatilsynet ytterligere informasjon fra Trumf, hvorav Trumf informerte at implementeringen av verifikasjonsløsningen deres gikk som planlagt. Sakens faktiske omstendigheter ble følgelig først, i det vesentlige, avklart i juni 2021, jf. PVN-2021-03.

Datatilsynet mener at sakens fremdrift og saksbehandlingstiden for øvrig ikke skal utgjøre en formildende omstendighet i denne saken. Den lengste inaktiviteten har vært på rundt 5 måneder, fra sakens faktiske omstendigheter ble i det vesentlige avklart frem til varsel om vedtak. Sakens betydning og omfang innebærer at 5 måneder ikke er uakseptabel lang tid. Videre har det gått 6 måneder fra Trumf ga sine merknader til dette vedtaket er truffet. Heller ikke dette kan anses for å være uakseptabelt.

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

6.3. Vurdering av gebyrets størrelse

Ved utmåling av gebyrets størrelse skal det legges vekt på de samme vurderingsmomentene som i spørsmålet om hvorvidt gebyr bør ilegges. Vi viser derfor til vurderingene av sakens alvorlighet ovenfor. Overtredelsesgebyret skal være virkningsfullt, stå i et rimelig forhold til overtredelsen og virke avskrekkende. Dette innebærer at tilsynsmyndigheten skal gjøre en konkret, skjønnsmessig vurdering i hvert enkelt tilfelle.

14 HR-2016-225-S, avsnitt 32.

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

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

Av kommentarutgaven, i relasjon til artikkel 83, fremgår det:

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

Og videre:

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

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

Det har blitt konkludert med at Trumf brøt sine forpliktelser etter artikkel 32, artikkel 33 nr. 1 og artikkel 33 nr. 5. Trumf sendte ikke meldinger til tilsynsmyndighetene om brudd på personopplysningssikkerheten og implementerte for øvrig ikke egnede sikkerhetstiltak, til tross for at det var klart – på bakgrunn av sakens omstendigheter – at Datatilsynet var meget tydelige på behovet for å verifisere kontohavere. Datatilsynet var klare på dette behovet, blant annet, på grunn av misbrukspotensialet som lå i at informasjon om kontohavere ble tilgjengelig for Trumf-medlemmer.

Etter artikkel 83 nr. 4 kan det ilegges et overtredelsesgebyr på opptil 10 000 000 euro eller, dersom det dreier seg om et «foretak» («undertaking» på engelsk) på opptil 2% av den samlede globale årsomsetningen i forutgående regnskapsår, der det høyeste beløpet anvendes. I fortalepunkt 150 bemerkes følgende:

> *Dersom et foretak ilegges overtredelsesgebyr, bør et foretak for disse formål forstås som et foretak i henhold til artikkel 101 og 102 i TEUV.*

EU-domstolen har, blant annet i C-231/11 P - C-233/11, gitt følgende bemerkninger knyttet til forståelsen av «foretak», men da i annen rettslig kontekst:

> *The authors of the Treaties chose to use the concept of an undertaking to designate the perpetrator of an infringement of competition law, who is liable to be punished pursuant to*

Articles 81 EC and 82 EC, and not other concepts such as the concept of a company or firm or of a legal person, used, inter alia, in Article 48 EC (see, to that effect, Case C-501/11 P Schindler Holding and Others v Commission [2013] ECR, paragraph 102).

The Court of Justice has consistently held that the concept of an undertaking covers any entity engaged in an economic activity, regardless of the legal status of the entity or the way in which it is financed. That concept must be understood as covering an economic unit, even if, from a legal perspective, that unit is made up of a number of natural or legal persons (see, inter alia, Joined Cases C-628/10 P and C-141/11 P Alliance One International and Standard Commercial Tobacco v Commission [2012] ECR, paragraph 42 and the case-law cited).

I «The EU General Data Protection Regulation, GDPR, A Commentary», side 1187-1188, gis det følgende kommentar til artikkel 83:

Articles 101 and 102 TFEU do not themselves contain any definition of the concept of 'undertaking'. Consequently, the reference in recital 150 should be understood as a reference to the whole body of jurisprudence concerning the definition of an 'undertaking' under the TFEU.

In this respect, the case law of the EU courts in the area of competition law has defined an undertaking as an economic unit, which may comprise several natural or legal persons or 'which may be formed by the parent company and all involved subsidiaries', together referred to as a 'single economic entity'. Moreover, under this case law, each person forming part of a single economic entity may be held liable for an infringement of EU competition law committed by that economic entity.[15]

I henhold til Proff er NorgesGruppen Forbrukerservice AS eneste aksjonær i Trumf. NorgesGruppen Forbrukerservice AS er eid av NorgesGruppen ASA. På denne bakgrunn legger vi til grunn at Trumf AS og NorgesGruppen ASA inngår i samme «foretak», jf. artikkel 83 nr. 4, og omsetningen til NorgesGruppen ASA må tas i betraktning ved utmålingen av overtredelsesgebyret.

Årsresultatet for NorgesGruppen ASA, for 2020, viser en omsetning på 101,56 milliarder kroner, en oppgang fra 90,5 milliarder kroner i 2019.[16]

Gebyret skal settes så høyt at det er virkningsfullt og oppnår tilstrekkelig avskrekkende effekt. Utfra virksomhetens høye omsetning, samt de alvorlige bruddene på personvernforordningen i saken, har vi kommet frem til at et overtredelsesgebyr på kr 5 000 000 anses riktig. Beløpet utgjør ca. 0,005 prosent av virksomhetens omsetning i forrige regnskapsår.

Overtredelsesgebyret ligger følgelig helt i nederste sjikt av hva personvernforordningen artikkel 83 nr. 3 gir Datatilsynet kompetanse til å ilegge.

7. Klagerett og videre saksgang

15 THE EU GENERAL DATA PROTECTION REGULATION (GDPR), A Commentary, redigert av Kuner, Bygrave og Docksey, 2020.

16 https://www.dn.no/handel/norgesgruppen/kiwi/meny/rekordar-for-koronavinneren-norgesgruppen-over-100-milliarder-i-omsetning/2-1-986439 og https://www.norgesgruppen.no/globalassets/finansiell-informasjon/rapporter/2020/ars-og-barekraftsrapport-2020.pdf.

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.

8. 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.

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

Med vennlig hilsen

Jørgen Skorstad
avdelingsdirektør, jus

Ida Småge Breidablikk
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

false