

Styrets leder på vegne av styret
TELENOR ASA
Postboks 800
1331 FORNEBU

Deres referanse
[WSWR-
LEGAL.FID1258636]

Vår referanse
21/03823-45

Dato
10.03.2025

Vedtak - Personvernombudets rolle i Telenor ASA

1	Innledning og sammendrag	3
2	Vedtak	3
3	Sakens bakgrunn	4
4	Rettslig bakgrunn	6
4.1	Tilsynsmyndighetenes kompetanse, oppgaver og myndighet i henhold til personvernforordningen	6
4.2	EØS-retten og norsk lov	9
5	Utpeking av personvernombud, personvernforordningen artikkel 37	9
5.1	Tilsynskriterier og tilsynsbevis	9
5.2	Datatilsynets vurdering	11
5.2.1	Om utpekelse av personvernombud	11
5.2.2	Om plikten til å føre behandlingsprotokoll etter personvernforordningen artikkel 30	14
5.2.3	Om innholdet i behandlingsprotokollen inkludert Telenor ASAs rolle og ansvarsfordeling	15
5.2.4	Angående kontaktopplysninger	22
5.2.5	Konklusjon	23
6	Involvering av personvernombud, personvernforordningen artikkel 38 nr. 1	23
6.1	Tilsynskriterier og tilsynsbevis	23
6.2	Datatilsynets vurdering	24
7	Tildeling av ressurser, personvernforordningen artikkel 38 nr. 2	27
7.1	Tilsynskriterier og tilsynsbevis	27

7.2	Datatilsynets vurdering.....	27
8	Personvernombudets tilgang til øverste ledelse, personvernforordningen artikkel 38 nr. 3.....	31
8.1	Tilsynskriterier og tilsynsbevis.....	31
8.2	Datatilsynets vurdering.....	31
9	De registrertes tilgang til personvernombudet, artikkel 38 nr. 4	41
9.1	Tilsynskriterier og tilsynsbevis.....	41
9.2	Datatilsynets vurdering.....	42
10	Personvernombudets uavhengighet og fravær av interessekonflikter, artikkel 38 nr. 3 og 6.....	42
10.1	Tilsynskriterier og tilsynsbevis	42
10.2	Datatilsynets vurdering	42
11	Personvernombudets oppgaver, artikkel 39 nr. 1	51
11.1	Tilsynskriterier og tilsynsbevis	51
11.2	Datatilsynets vurdering	52
12	Organisatoriske tiltak for å sikre overholdelse av artikkel 24 nr. 1 og 2.....	52
12.1	Tilsynskriterier og tilsynsbevis	52
12.2	Datatilsynets vurdering	52
12.2.1	Omfanget av behandlingsansvar.....	53
12.2.2	Angående organisatoriske tiltak	56
13	Vurdering av korrigerende tiltak	64
13.1	Oppsummering av konklusjoner med hensyn til korrigerende tiltak.....	64
13.2	Pålegg om tiltak.....	65
13.3	Irettesettelse.....	67
13.4	Vurdering av om det skal ilegges overtredelsesgebyr	68
13.4.1	Generelle prinsipper ved vurdering av overtredelsesgebyr	68
13.4.2	Lovkrav	69
13.4.3	Momenter som skal tillegges særskilt vekt ved vurdering av gebyr.....	70
13.4.4	Konklusjon om hvorvidt det skal ilegges overtredelsesgebyr	75
13.5	Fastsettelse av overtredelsesgebyr.....	75
14	Inndrivelse av overtredelsesgebyr	77
15	Europeisk samarbeid	77
16	Adgang til dokumenter	78
17	Klageadgang	78

1 Innledning og sammendrag

Datatilsynet (heretter også «vi», «vår», «oss», «tilsynsmyndigheten») er kompetent tilsynsmyndighet i henhold til lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven) § 20 nr. 1 og artikkel 51 i *Europaparlaments- og rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF* (personvernforordningen, heretter også kalt «GDPR»).

Vi fatter herved et vedtak om å utstede et pålegg, ilegge en irettesettelse og ilegge et overtredelsesgebyr til Telenor ASA¹ (heretter også nevnt «den behandlingsansvarlige», «databehandleren», «selskapet», «foretaket», «parten», «arbeidsgiveren», «dere» og «deres») av årsaker som vil beskrives nedenfor. Telenor ASA er adskilt fra Telenor Group (heretter også nevnt «konsernet» og «gruppen»), som består av morselskapet og datterselskaper (heretter også kalt «forretningsenheter»).

Andre berørte tilsynsmyndigheter, i de EØS land hvor Telenor har forretningsenheter (Danmark, Sverige og Finland), ble konsultert før vedtaket ble fattet.

Utdrag fra dokumenter som ikke foreligger på norsk er gjengitt i originalspråket. Dette inkluderer Telenor ASAs interne dokumenter og stillingstitler. For dokumenter fra EU-organer brukes i utgangspunktet dansk språkversjon, sekundært engelsk.

Sammendrag

Etter å ha mottatt anonyme tips, innledet Datatilsynet et tilsyn med Telenor ASAs overholdelse av kravene til personvernombud fastsatt i personvernforordningen artikkel 37–39 og kravene til organisatoriske tiltak fastsatt i personvernforordningen artikkel 24. Basert på tilsynet konkluderer vi at Telenor ASA har overtrådt personvernforordningen artikkel 37 nr. 7, artikkel 38 nr. 2 og 3 og artikkel 24 nr. 1 og nr. 2 i tilsynsperioden. Som følge av tilsynet ilegger vi Telenor ASA pålegg, irettesettelse og et overtredelsesgebyr, som nærmere beskrevet i punkt 2.

2 Vedtak

I medhold av personvernforordningen artikkel 58 nr. 2 bokstav d, jf. personvernforordningen artikkel 24 nr. 1 og 2, ilegger vi følgende pålegg til Telenor ASA:

- *Å lage en dokumentert intern analyse om hvorvidt Telenor ASA er forpliktet å utpeke personvernombud som tar bl.a. hensyn til Telenor ASAs rolle i de forskjellige behandlingsaktiviteter.*
- *Å revidere behandlingsprotokollen etter personvernforordningen artikkel 30 og iverksette organisatoriske tiltak for å sikre at den til enhver tid gir en oppdatert*

¹ Telenor ASA er morselskapet i Telenor konsernet.

beskrivelse av behandlingsaktivitetene i Telenor ASA, antall registrerte og rollene Telenor ASA har.

- *I tilfelle Telenor ASA faktisk er forpliktet til å ha et personvernombud, å gjennomføre organisatoriske tiltak og innføre egnede retningslinjer med hensyn til personvernombudets organisering. Dette inkluderer beskrivelse av rapporteringslinje til tydelig definert øverste ledelsesnivå, beskrivelse av hvilke oppgaver personvernombudet bør involveres i, samt på hvilken måte og hva som er rett tid. Vurderinger og tiltak for å sikre uavhengighet og at det ikke foreligger interessekonflikter inkluderer å skille klart mellom eventuelle andre roller i stillingsbeskrivelse, sørge for egen e-postadresse for personvernombudet og gjøre en dokumentert vurdering av ombudets aksjeeierskap i selskapet.*

I henhold til personvernforordningen artikkel 58 nr. 2 bokstav b, jf. personvernforordningen artikkel 38 nr. 3 siste punktum, ilegger vi Telenor ASA irettesettelse for

- *å ikke ha på plass rapporteringslinje for personvernombudet i Telenor ASA til øverste ledelsesnivå for ca. ett år av tilsynsperioden.*

*I henhold til personvernforordningen artikkel 58 nr. 2 bokstav i og personopplysningsloven § 26 ilegger vi Telenor ASA et overtredelsesgebyr på **NOK 4 000 000** for*

- *å ikke ha gjennomført egnede organisatoriske tiltak for å sikre og kunne påvise overholdelse av personvernforordningen, i strid med artikkel 24 nr. 1, og ikke å ha innført egnede retningslinjer for vern av personopplysninger, i strid med personvernforordningen artikkel 24 nr. 2.*

3 Sakens bakgrunn

Datatilsynets ledelse bestemte i 2021 å gjennomføre et stedlig tilsyn hos Telenor ASA. Forholdene tilsynet skulle avklare, var Telenor ASAs overholdelse av kravene til personvernombud fastsatt i personvernforordningen artikkel 37–39 og krav til egnede organisatoriske tiltak fastsatt i artikkel 24.

Stedlig tilsyn var opprinnelig planlagt gjennomført hos Telenor ASA 7. januar 2022. På grunn av regjeringens restriksjoner knyttet til Covid-19-pandemien, måtte imidlertid tilsynet utsettes til 28. januar 2022, da Datatilsynet gjennomførte flere intervjuer med ledere og ansatte i Telenor ASA via videokonferanse. Tilsynet og intervjuene gjaldt faktiske forhold i perioden fra 10. oktober 2020² til intervjuene ble gjennomført 28. januar 2022 (heretter omtalt som «tilsynsperioden»).

² Datoen da daværende personvernombud [REDACTED] ble meldt til Datatilsynet som personvernombud for første gang. Se den endelige tilsynsrapporten av 30. september 2022, s. 2.

I vårt tilsynsvarsel datert 26. november 2021 ba vi Telenor ASA om konkret dokumentasjon, som vi mottok 13. desember 2021. Vi ba også om ytterligere dokumentasjon 22. desember 2021, som vi mottok 9. januar 2022. Etter intervjuene 28. januar 2022 ba vi videre Telenor ASA om å dele sin behandlingsprotokoll, som vi mottok 2. februar 2022. Vi sendte vår foreløpige tilsynsrapport til Telenor ASA den 11. april 2022 og mottok merknader 16. mai 2022. Telenor ASAs merknader er omtalt og innarbeidet i den endelige tilsynsrapporten.

For nærmere opplysninger om den faktiske bakgrunnen for den foreliggende sak viser vi til vår endelige tilsynsrapport datert 30. september 2022.

Datatilsynet fikk ny direktør, Line Coll, 1. august 2022. Sommeren 2023 konkluderte Coll med at hun var inhabil i saken på grunn av sin tidligere rolle som partner i advokatfirmaet Wikborg Rein, der hun hadde gitt Telenor ASA juridisk rådgivning i forbindelse med Datatilsynets tilsyn. Det ble sendt forespørsel til Kommunal- og regionaldepartementet om å oppnevne en stedfortredende direktør for saken. Departementet kom den 20. november 2023 frem til at Coll var inhabil i saken. I henhold til forvaltningsloven § 6 tredje ledd kan avgjørelse i saken ikke treffes av en direkte underordnet tjenestemann i Datatilsynet når den overordnede tjenestemannen er inhabil. I henhold til teori og tolkningen av ordlyden i forvaltningsloven § 6 tredje ledd kan imidlertid Datatilsynets ansatte bistå i saksbehandlingen og utarbeidelsen av avgjørelser.

Departementet oppnevnte Mona Naomi Lintvedt som stedfortredende direktør for denne saken, og avgjørelser i saken ble gjort under hennes ledelse. Ettersom den endelige tilsynsrapporten ble ferdigstilt etter at Coll tiltrådte, har stedfortredende direktør vurdert om inhabiliteten vil påvirke rapportens gyldighet. I en vurdering datert 30. desember 2023 konkluderte hun med at den endelige rapporten ikke inneholdt noen vurderinger eller vedtak, men bare beskrev fakta og funn fra tilsynet, og derfor ikke var berørt av inhabiliteten til Datatilsynets direktør og ansatte.

Forhåndsvarsel ble gitt 1. mars 2024 i samsvar med forvaltningsloven § 16 («forhåndsvarsling»)³ for å gi selskapet mulighet til å uttale seg skriftlig i saken før vedtak ble truffet.

Datatilsynet anser dette som en grenseoverskridende sak der samarbeidsmekanismen i personvernforordningen artikkel 60 kommer til anvendelse, noe som innebærer at et utkast til vedtaket ble delt med de aktuelle tilsynsmyndighetene i EØS.⁴ Se videre punkt 4.1. På grunn av ovennevnt europeisk samarbeid og at Telenor ASAs arbeidsspråk er engelsk, ble forhåndsvarselet opprinnelig skrevet på engelsk. På forespørsel fra Telenors ASAs advokat utarbeidet vi norsk versjon av varselet som ble sendt til selskapet 18. april 2024. Ved motstrid legges den norske teksten til grunn. Wikborg Rein på vegne av Telenor ASA leverte sine merknader til forhåndsvarselet 31. mai 2024 (heretter også omtalt som «tilsvaret»).

³ Lov av 10. februar 1967 om behandlingsmåten i forvaltningssaker (forvaltningsloven).

⁴ Det europeiske økonomiske samarbeidsområdet

4 Rettslig bakgrunn

4.1 Tilsynsmyndighetenes kompetanse, oppgaver og myndighet i henhold til personvernforordningen

Vi viser til personvernforordningen artikkel 55 nr. 1, artikkel 56 nr. 1 og artikkel 58 nr. 2 om Datatilsynets kompetanse, oppgaver og myndighet. Vi viser videre til personvernforordningen artikkel 83 nr. 1 til 5 om ilegging av overtredelsesgebyr og personopplysningsloven § 26 første ledd.

Personvernforordningen artikkel 3 nr. 1 lyder slik:

«Denne forordning får anvendelse på behandling av personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten til en behandlingsansvarlig eller en databehandler i Unionen, uavhengig av om behandlingen finner sted i Unionen eller ikke.»

Telenor Group har virksomhet og forretningsenheter/kontorer («Business Units» (BU)) både i og utenfor EØS:

«The Telenor Group (of companies) consists of several autonomous legal entities, registered both in Norway and across the globe, with separate Boards of Directors. This includes the administrative headquarters and Group parent company Telenor ASA, and various ‘Business Units’ (BUs) which are subsidiaries directly or indirectly controlled by Telenor ASA».⁵

I henhold til personvernforordningen artikkel 3 nr. 1 vil forordningen komme til anvendelse for all behandling av personopplysninger i Telenor ASA, hvor selskapet opptrer som behandlingsansvarlig, felles behandlingsansvarlig og/eller databehandler, uansett om behandlingsaktivitetene foregår i eller utenfor EØS.

Med hensyn til behandlingsaktivitetene som omfattes av tilsynet, regnes Telenor ASA som behandlingsansvarlig (jf. personvernforordningen artikkel 4 nr. 7) eller databehandler (jf. personvernforordningen artikkel 4 nr. 8), avhengig av den aktuelle behandlingen.⁶ Som behandlingsansvarlig og databehandler har Telenor ASA sin hovedvirksomhet i Norge, jf. personvernforordningen artikkel 4 nr. 16.

Vi anser at behandlingsaktiviteter som omfattes av den foreliggende saken, er å regne som «grenseoverskridende behandling» i henhold til personvernforordningen artikkel 4 nr. 23. Telenor ASA hevder i sine merknader til forhåndsvarsel at saken ikke er av grenseoverskridende karakter fordi saken ikke gjelder bestemte behandlingsaktiviteter og – subsidiært – fordi behandlingen ikke oppfyller kravet i personvernforordningen artikkel 4 nr.

⁵ «Response to Datatilsynet», 13.12.2021 s. 1.

⁶ «Response to Datatilsynet», 13.12.2021, s. 1.

23 bokstav b, særlling vilkåret om å påvirke registrerte i mer enn én medlemsstat «i betydelig grad».⁷

Vi har vurdert Telenor ASAs argumentasjon, men fastholder vår vurdering som vi utdyper nærmere i det følgende.

Først og fremst bør det fremheves at – siden personvernombudet må involveres i «alle» spørsmål som gjelder vern av personopplysninger, jf. personvernforordningen artikkel 38 nr. 1 – er det *all* behandling av personopplysninger som finner sted i forbindelse med aktiviteter i Telenor ASA som omfattes av den foreliggende saken. Dokumentasjonen som Telenor ASA har tilsendt Datatilsynet viser at et bredt spekter av behandlingsaktiviteter finner sted i forbindelse med aktiviteter i Telenor ASA i Norge og i andre land, i og utenfor EØS. Behandlingsprotokollen viser til flere «countries of processing» i EØS (Danmark, Sverige, Finland m.fl).⁸ Flere av disse behandlingsaktivitetene gjelder faktisk data til ansatte i hele Telenor-konsernet, og finner derfor sted i forbindelse med aktiviteter i flere Telenor-forretningssenheter i og utenfor EØS. Dette oppfyller i seg selv kravet i artikkel 4 nr. 23 bokstav a.

Vi bemerker at i personvernforordningens forstand, innebærer en «virksomhet» (eller etablering («establishment»)) «en effektiv og faktisk utøvelse av aktivitet gjennom en stabil struktur. En slik strukturs rettslige form, enten det dreier seg om en filial eller et datterforetak med status som juridisk person, er ikke av avgjørende betydning i denne forbindelse».⁹ Med andre ord dekker begrepet «virksomhet» ikke bare stedet for den formelle innlemmelsen til behandlingsansvarlig eller databehandler; det dekker også datterselskaper, filialer og agenter i utlandet, som for eksempel «all Telenor companies» i EØS, jf. kolonnen «recipients of personal data» i behandlingsprotokollen. Derfor mener vi det ikke er korrekt slik det er hevdet i tilsvaret at «[g]itt at Telenor ASA kun er etablert i Norge, er det eventuelt bestemmelsen i bokstav b som kan danne grunnlag for å karakterisere behandlingen som grenseoverskridende».¹⁰ Telenor ASA har – i personvernforordningens forstand – flere etableringer i EØS, og derfor er det ikke bare bestemmelsen i bokstav b som kan danne grunnlag for å karakterisere behandlingen.

I tillegg, for å anse at behandlingen finner sted «i forbindelse med aktiviteter i» en behandlingsansvarliges eller databehandlers virksomhet, trenger den ikke å utføres direkte av den virksomheten¹¹. Det er nok at behandlingen er knyttet til aktivitetene til den virksomheten. Følgelig er vilkåret i personvernforordningen artikkel 4 nr. 23 bokstav a oppfylt med hensyn til behandlingsaktivitetene som beskrives i behandlingsprotokollen med flere EØS-land («countries of procesing») eller som involverer Telenors datterselskaper eller

⁷ Merknader til forhåndsvarsel av 31.mai 2024, s. 21-24.

⁸ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

⁹ Personvernforordningen fortalepunkt 22 og EU-domstolen sak C-191/15, *Verein für Konsumenteninformation*, avsnitt 75-76.

¹⁰ Merknader til forhåndsvarsel av 31.mai 2024, s. 22.

¹¹ EU-domstolen sak C-131/12, *Google Spain*, avsnitt 52-53 og EU-domstolen sak C-230/14, *Weltimmo*, avsnitt 25 og 35.

filialer i EØS, slik som hva gjelder ansatte på tvers av Telenor-konsernet (og ikke bare ansatte i Telenor ASA).¹²

Dessuten er det behandlingsaktiviteter som finner sted i forbindelse med etableringen i Norge, men som i betydelig grad påvirker eller sannsynligvis vil påvirke registrerte i flere EØS-land. Dette er for eksempel tilfelle med hensyn til «multi-year surveys in Telenor's markets to understand customer behaviours» som i henhold til behandlingsprotokollen påvirker [REDACTED] kunder i flere EØS-land gjennom en analyse av deres atferd som kan være spesielt påtrengende. Det samme gjelder når behandlingsaktiviteter i Norge påvirker alle ansatte i Telenor-konsernet som for eksempel «Learning Management systems» og «Employee Share Plan», som i henhold til behandlingsprotokollen påvirker [REDACTED] registrerte. Det kommer frem i vår endelige tilsynsrapport at antall ansatte i Telenor konsernet i tilsynperioden er ca 15 000.¹³ I denne forbindelse må det bemerkes at konsistensmekanismen for samarbeid mellom tilsynsmyndighetene gjelder når behandlingsaktiviteter i vesentlig grad berører et *betydelig antall* registrerte i flere EØS-land, jf. personbefordringen fortalepunkt 135. Vi anser at vilkåret om et betydelig antall er oppfylt. Vi understreker at vilkåret om å påvirke registrerte *i betydelig grad* ikke er et krav etter personvernforordningen artikkel 4 nr. 23 bokstav a, men kun under bokstav b, og at det derfor ikke strengt tatt er nødvendig å påvise at kravet er oppfylt i denne saken. Uansett er terskelen lav for hva som anses å *i betydelig grad* påvirke registrerte. EDPBs veiledning legger for eksempel til grunn at det er tilstrekkelig dersom den aktuelle behandlingen påvirker eller sannsynligvis vil påvirke enkeltpersoners «sundhed, trivsel og ro i sindet».¹⁴

Dokumentasjonen innsamlet av Datatilsynet har videre vist at Telenor ASA har interne rutiner og retningslinjer¹⁵ som er de samme i alle land Telenor Group opererer i, og dermed påvirker registrerte i flere EØS-land. Vi forutsetter at Telenor ASA som morselskap og behandlingsansvarlig har myndighet til å endre og påvirke konsernets retningslinjer.¹⁶ Tilsynet har avdekket at Telenor ASA, i tillegg til å være behandlingsansvarlig for behandling av visse personopplysninger, noen ganger fungerer som databehandler på vegne av andre forretningsenheter og også kan fungere som felles behandlingsansvarlig med andre forretningsenheter, noe som i seg selv innebærer et grenseoverskridende element.¹⁷

Samarbeidsmekanismen og prosedyren fastsatt i personvernforordningen artikkel 56 nr. 1 og artikkel 60 kommer derfor til anvendelse i denne saken. Datatilsynet har kompetanse til å opptre som ledende tilsynsmyndighet i saken etter artikkel 56 nr. 1. I henhold til

¹² I denne forbindelse bør det bemerkes at når behandlingsprotokollen refererer til behandling av ansattes data, refererer det til flere tusen ansatte. Det er derfor åpenbart ikke bare de ansatte i Telenor ASA, jf. kolonner «data subject categories» og «number of data subjects» i behandlingsprotokollen.

¹³ Endelig tilsynsrapport av 30. september 2022, s. 11,

¹⁴ Retningslinjer 08/2022 for udpegelse af en ledende tilsynsmyndighed for en dataansvarlig eller databehandler, versjon 2.0, vedtatt 28.3.2023, s. 5.

¹⁵ Group Manual Privacy

¹⁶ I «Response to Datatilsynet», 13.12.2021 s. 1 står: «The Telenor Group (of companies) consists of several autonomous legal entities, registered both in Norway and across the globe, with separate Boards of Directors. This includes the administrative headquarters and Group parent company Telenor ASA, and various 'Business Units' (BUs) which are subsidiaries directly or indirectly controlled by Telenor ASA»

¹⁷ Endelig tilsynsrapport av 30. september 2022, s. 6.

personvernforordningen artikkel 60 skal Datatilsynet samarbeide med de andre berørte tilsynsmyndighetene. Dette innebærer å utveksle relevant informasjon om saken og legge frem utkast til avgjørelse for de andre berørte tilsynsmyndighetene slik at de kan avgi en uttalelse. Det skal tas behørig hensyn til deres synspunkter ved avgjørelse av saken.

4.2 EØS-retten og norsk lov

Personvernforordningen er innlemmet i vedlegg XI til avtalen om Det europeiske økonomiske samarbeidsområde («EØS-avtalen») ved EØS-komiteens beslutning nr. 154/2018 («EØS-komiteens beslutning»)¹⁸.

Artikkel 1 bokstav b i EØS-komiteens beslutning fastsetter at:

«[...] betydningen av ordene ‘medlemsstat(er)’ og ‘tilsynsmyndigheter’ [skal] også omfatte, i tillegg til den betydning de har i forordningen, henholdsvis EFTA-statene og deres tilsynsmyndigheter.»

Videre lyder EØS-komiteens beslutning artikkel 1 bokstav c som følger:

«Henvvisninger til unionsretten eller Unionens bestemmelser om vern av personopplysninger skal forstås som henvisninger til henholdsvis EØS-avtalen eller dens bestemmelser om vern av personopplysninger.»

Personopplysningsloven innlemmet personvernforordningen i norsk rett. Personopplysningsloven og personvernforordningen trådte i kraft i Norge 20. juli 2018.

5 Utpeking av personvernombud, personvernforordningen artikkel 37

5.1 Tilsynskriterier og tilsynsbevis

Personvernforordningen artikkel 37 lyder som følger:

- 1) Den behandlingsansvarlige og databehandleren skal utpeke et personvernombud når
 - a) behandlingen utføres av en offentlig myndighet eller et offentlig organ, bortsett fra domstoler som opptrer innenfor rammen av sin domsmyndighet,
 - b) den behandlingsansvarliges eller databehandlerens kjernevirksomhet består av behandlingsaktiviteter som på grunn av sin art, sitt omfang og/eller formål krever regelmessig og systematisk monitorering i stor skala av registrerte, eller

¹⁸ EØS-komiteens beslutning nr. 154/2018 av 6. juli 2018 om endring av EØS-avtalens vedlegg XI (Elektronisk kommunikasjon, audiovisuelle tjenester og informasjonssamfunnstjenester) og protokoll 37 om listen omhandlet i artikkel 101, EUT [2018] L 183/23.

- c) den behandlingsansvarliges eller databehandlerens kjernevirksomhet består av behandling i stor skala av særlige kategorier av opplysninger i medhold av artikkel 9 eller personopplysninger om straffedommer og lovovertridelser som nevnt i artikkel 10.
- 2) Et konsern kan utnevne ett personvernombud, forutsatt at alle virksomhetene har enkel tilgang til vedkommende.
 - 3) Dersom den behandlingsansvarlige eller databehandleren er en offentlig myndighet eller et offentlig organ, kan det utpekes ett personvernombud for flere av nevnte myndigheter eller organer, idet det tas hensyn til deres organisasjonsstruktur og størrelse.
 - 4) I andre tilfeller enn dem nevnt i nr. 1 kan eller, dersom det kreves i unionsretten eller i medlemsstatenes nasjonale rett, skal den behandlingsansvarlige eller databehandleren eller sammenslutninger og andre organer som representerer kategorier av behandlingsansvarlige eller databehandlere, utpeke et personvernombud. Personvernombudet kan handle på vegne av nevnte sammenslutninger og andre organer som representerer behandlingsansvarlige eller databehandlere.
 - 5) Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner og særlig på grunnlag av dybdekunnskap om personvernlovgivning og praksis på området samt evne til å utføre oppgavene nevnt i artikkel 39.
 - 6) Personvernombudet kan være en ansatt hos den behandlingsansvarlige eller databehandleren eller utføre oppgavene på grunnlag av en tjenesteavtale.
 - 7) Den behandlingsansvarlige eller databehandleren skal offentliggjøre kontaktopplysningene til personvernombudet og meddele disse til tilsynsmyndigheten.

Vi viser videre til punkt 3.1.1 og 3.1.2 i den endelige tilsynsrapporten av 30. september 2022.

Personvernforordningen artikkel 30 lyder som følger:

- 1) Hver behandlingsansvarlig og, dersom det er relevant, den behandlingsansvarliges representant skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar. Nevnte protokoll skal inneholde følgende informasjon:
 - a. navnet på og kontaktopplysningene til den behandlingsansvarlige og, dersom det er relevant, den felles behandlingsansvarlige, den behandlingsansvarliges representant og personvernombudet,
 - b. formålene med behandlingen,
 - c. en beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger,
 - d. kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, herunder mottakere i tredjestater eller internasjonale organisasjoner,

- e. dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredje stat eller internasjonale organisasjon og, ved overføringer nevnt i artikkel 49 nr. 1 annet ledd, dokumentasjon på nødvendige garantier,
 - f. dersom det er mulig, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger,
 - g. dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1.
- 2) Hver databehandler og, dersom det er relevant, databehandlerens representant skal føre en protokoll over alle kategorier av behandlingsaktiviteter som er utført på vegne av en behandlingsansvarlig, og som skal inneholde:
- a. navnet på og kontaktopplysningene til databehandleren eller databehandlerne og til hver behandlingsansvarlig som databehandleren opptrer på vegne av, samt, dersom det er relevant, den behandlingsansvarliges eller databehandlerens representant og personvernombudet,
 - b. kategoriene av behandling utført på vegne av hver behandlingsansvarlig,
 - c. dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredje stat eller internasjonale organisasjon og, ved overføringer nevnt i artikkel 49 nr. 1 annet ledd, dokumentasjon på nødvendige garantier
 - d. dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1.
- 3) Protokollene nevnt i nr. 1 og 2 skal være skriftlige, herunder elektroniske.
- 4) Den behandlingsansvarlige eller databehandleren og, dersom det er relevant, den Den behandlingsansvarliges eller databehandlerens representant skal på anmodning gjøre protokollen tilgjengelig for tilsynsmyndigheten.
- 5) Forpliktelsene nevnt i nr. 1 og 2 gjelder ikke et foretak eller en organisasjon med færre enn 250 ansatte, med mindre behandlingen det/den utfører, sannsynligvis vil medføre en risiko for de registrertes rettigheter og friheter, behandlingen ikke skjer leilighetsvis eller omfatter særlige kategorier av opplysninger som nevnt i artikkel 9 nr. 1 eller personopplysninger om straffedommer og lovovertridelser nevnt i artikkel 10.

5.2 Datatilsynets vurdering

5.2.1 Om utpekelse av personvernombud

I hele tilsynsperioden hadde Telenor ASA utnevnt et kvalifisert personvernombud i henhold til personvernforordningen artikkel 37 nr. 5, og kontaktopplysningene var formidlet til Datatilsynet. Dette er ubestridt.

Under tilsynet var det ikke et tema hvorvidt Telenor ASA falt innenfor artikkel 37 nr. 1 hvor oppnevning av personvernombud er obligatorisk eller om det var en frivillig ordning. Dette ble derfor heller ikke drøftet videre i tilsynsrapport eller varsel om vedtak. Det ble lagt til

grunn i saken at Telenor ASA hadde oppnevnt et personvernombud, og da følger det av Personvernrådets veileder om personvernombud at kravene til rollen i artikkel 38 og 39 er tilsvarende som for tilfeller hvor ombudet er obligatorisk.¹⁹

Etter mottak av varsel om vedtak, opplyste Telenor ASA i brev 31. mai 2024, opphør av funksjonen som personvernombudet i selskapet fordi de mener at selskapets behandlingsaktiviteter ikke faller inn under krav om obligatorisk personvernombud i artikkel 37. Opphøret ble formelt meldt 11. juni 2024 til Datatilsynet. Telenor ASA redegjorde ikke nærmere for vurderinger av hvorfor det ikke anses som obligatorisk for selskapet å ha personvernombud, men legger dette til grunn uten videre dokumentasjon.

Vi bemerker det som står i Personvernrådets veileder om personvernombud:

«Når en organisation udpeger en databeskyttelsesrådgiver på frivillig basis, gælder kravene i henhold til artikel 37-39 for hans eller hendes udpegelse, stilling og opgaver, som hvis udpegelsen havde været obligatorisk.»²⁰

Vi vurderer at kravene i personvernforordningen art. 37-39 gjelder uansett i denne saken. Hvorvidt Telenor ASA er forpliktet til å ha et personvernombud eller ikke kan påvirke vurdering av sanksjoner, inkludert størrelsen på et overtredelsesgebyr.

I ovennevnt veiledning fremkommer videre:

«Medmindre det er indlysende, at en organisation ikke er forpligtet til at udpege en databeskyttelsesrådgiver, så anbefaler Artikel 29-gruppen, at dataansvarlige og databehandlere dokumenterer den interne analyse, som er udført med henblik på at bestemme, hvorvidt en databeskyttelsesrådgiver skal udpeges, for dermed at kunne demonstrere, at de relevante faktorer er blevet taget korrekt i betragtning.»²¹

Personvernrådet viser til personvernforordningen artikkel 24 nr. 1 i denne sammenhengen og fortsetter med:

«Denne analyse er en del af dokumentationen vedrørende ansvarlighedsprincippet.»²² jf. personvernforordningen artikkel 5 nr. 2.

I vårt varsel om stedlig tilsyn av 26. november 2021 ba vi spesifikt om dokumentasjon om utpeking av personvernombud som en del av internkontrollen jf. personvernforordningen artikkel 24 nr. 2.²³ En dokumentert intern analyse om på hvilket grunnlag personvernombudet

¹⁹ WP 243 rev.01 «Retningslinjer for databeskyttelsesrådgivere» vedtatt 13. desember 2016, senest revidert og vedtatt 5. april 2017, godkjent av EDPB i Endorsement 1/2018 av 25. mai 2018, s. 6.

²⁰ WP 243 rev.01 «Retningslinjer for databeskyttelsesrådgivere», s. 6.

²¹ WP 243 rev.01 «Retningslinjer for databeskyttelsesrådgivere», s. 5-6.

²² WP 243 rev.01 «Retningslinjer for databeskyttelsesrådgivere», s. 6.

²³ Forhåndsvarsel til vedtak av 18. april 2024, s. 2: «Datatilsynet ber om at følgende informasjon/dokumentasjon oversendes oss innen 13. desember 2021, jf. personvernforordningen artikkel 58 nr. 1:

b) Instruks/rutinebeskrivelser for følgende deler av internkontrollen, jf. personvernforordningen artikkel 24 nr. 2:

i Telenor ASA ble opprettet ble ikke levert til Datatilsynet, verken da eller på et senere tidspunkt. Dokumentasjonen er nødvendig for å kunne vise at dere har gjort en reell vurdering, der alle relevante faktorer har blitt tatt med. Dermed legger vi til grunn at en slik analyse ikke eksisterte. En slik analyse bør gjøres i henhold til ansvarsprinsippet med mindre det er åpenbart at selskapet ikke er forpliktet til å opprette et personvernombud – noe som ikke er åpenbart i dette tilfellet. Ikke på noe stadium under tilsynet, verken skriftlig eller muntlig, har dere nevnt eller påstått at dere mener at personvernombudet i Telenor ASA har operert på frivillig basis. Den påstanden kommer først i deres merknader til forhåndsvarsel. Hittil har vi oppfattet at det var enighet om at Telenor ASA er forpliktet til å ha et personvernombud, basert på opplysningene som Telenor ASA har gitt under tilsynet.

For å kunne svare på spørsmålet om Telenor ASA er forpliktet til å ha et personvernombud ifølge personvernforordningen artikkel 37 nr. 1 bokstav b må det ses hen til om kjernevirksomheten til Telenor ASA i sin rolle som behandlingsansvarlig eller databehandler, består av behandlingsaktiviteter som på grunn av sin art, sitt omfang og/eller formål krever regelmessig og systematisk monitorering i stor skala av registrerte. Telenor ASA hevder at selskapet ikke behandler «personopplysninger om ansatte på noen annen måte eller i noe større omfang enn det som er vanlig og nødvendig for andre virksomheter med ansatte. Behandlingene er knyttet til ansettelse, lønn, personaladministrasjon, opplæring og andre rutinemessige aktiviteter som krever håndtering av ansattes personopplysninger. Disse behandlingsaktivitetene utgjør nødvendige støttefunksjoner, og må betraktes som sideaktiviteter, ikke kjerneaktiviteter.»²⁴

Det er ubestridt at nødvendig personaladministrasjon og vanlig IT-støtte er standard i alle virksomheter og ikke blir sett på som kjernevirksomhet. Telenor ASA har for øvrig ikke gjort rede for hva deres kjernevirksomhet er.²⁵ I deres merknader av 31. mai 2024 beskrives selskapet som:

«et administrasjonsselskap med svært begrenset operasjonell aktivitet, med et begrenset antall kontoransatte og med i hovedsak lavrisiko behandlingsaktiviteter. Telenor ASA er ikke en telekomoperatør og leverer eller ikke slike tjenester til bedrifts- eller personkunder. Telenor ASA er i all hovedsak behandlingsansvarlig for behandlingen av personopplysninger om egne ansatte og for behandling av personopplysninger om egne leverandører mv., og har for øvrig en begrenset rolle som databehandler i enkelte relasjoner.»

Vi vil videre minne om at plikten til å oppnevne personvernombud ikke bare påhviler behandlingsansvarlig, men også databehandler. Telenor ASA må derfor ta hensyn til, ikke bare behandlingsaktiviteter selskapet utfører som behandlingsansvarlig, men også som databehandler i vurderingen av hvorvidt det foreligger plikt til å ha personvernombud. Alle

1) Utpeking av personvernombud.

2) Personvernombudets tilgang til virksomhetens ledelse.

3) Ledelsens involvering av personvernombudet for alle spørsmål som gjelder vern av personopplysninger.

4) Ledelsens gjennomgang av internkontroll.»

²⁴ Merknader til forhåndsvarsel av 31. mai 2024, s. 20.

²⁵ Merknader til forhåndsvarsel av 31. mai 2024, s. 12.

behandlingsaktiviteter²⁶ i virksomheten vurderes når det skal tas stilling til dette spørsmålet. Som det er redegjort nærmere for i neste punkt viser behandlingsprotokollen at det foregår langt flere behandlingsaktiviteter med større omfang enn rene HR-oppgaver i Telenor ASA. Etter vår vurdering er det ikke åpenbart at Telenor ASAs behandlingsaktiviteter er så begrenset som hevdet i tilsvaret. Tvert imot bekrefter tilsvaret at det finnes behandlingsaktiviteter i Telenor ASA som omfatter mer enn bare behandling av HR-data for ansatte i Telenor ASA, og at Telenor ASA også opptrer som databehandler.²⁷

Som vi vil komme tilbake til krever personvernforordningen artikkel 24 nr. 1 at den behandlingsansvarlige iverksetter organisatoriske tiltak for å sikre og påvise etterlevelse av loven, noe som krever en internkontroll.²⁸ Det er ubestridt i norsk litteratur at vurderingen om en virksomhet er forpliktet til å utpeke personvernombud skal dokumenteres og er en del av internkontrollen i personvernforordningen artikkel 24.²⁹ Dette er nødvendig for å sikre og påvise etterlevelse av reglene slik artikkel 24 krever. Når Telenor ASA ikke har kunnet fremlegge en slik dokumentert vurdering, er det altså et brudd på artikkel 24.

5.2.2 Om plikten til å føre behandlingsprotokoll etter personvernforordningen artikkel 30

Det er ubestridt at Telenor ASA har plikt til å føre behandlingsprotokoll etter personvernforordningen artikkel 30, og at de ikke faller innunder unntaket i artikkel 30 nr. 5 da virksomheten har flere enn 250 ansatte. I behandlingsprotokollen skal det blant annet gis informasjon som beskrivelse av formål, kategorier av personopplysninger, kategorier av registrerte og rollen til Telenor ASA som behandlingsansvarlig, felles behandlingsansvarlig og/eller databehandler. Datatilsynet ba om å få tilsendt en kopi av behandlingsprotokollen på slutten av tilsynsdagen 28. januar 2022. Telenor ASA sendte oss protokollen i e-post av 2. februar 2022, uten noen forbehold.

Telenor ASA gjør et poeng av at behandlingsprotokollen «ble etterspurt av Datatilsynet først i oppsummeringsmøtet helt på slutten av tilsynsdagen»³⁰ og «Protokollen var ikke tema da tilsynet ble gjennomført.»³¹ Telenor ASA påstår videre at opplysningene i behandlingsprotokollen dermed heller ikke vært gjenstand for kontradiksjon og at «selskapets forsøk på å forklare hva som skjer av behandlingsaktiviteter i Telenor ASA har ikke blitt fulgt opp av Datatilsynet.»³²

Datatilsynet mener dette ikke stemmer, og at Telenor ASA har fått flere anledninger til kontradiksjon i henhold til forvaltningsloven § 17.

²⁶ Se hen til personvernforordningen artikkel 38 nr. 1 om involvering av personvernombud i *alle* spørsmål som gjelder personvern og artikkel 4 punkt 2 som definerer «behandling».

²⁷ Merknader til forhåndsvarsel av 31.mai 2024, s. 14-18.

²⁸ Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2019) s. 273

²⁹ Jarbekk m.fl. s. 256-257.

³⁰ Merknader til forhåndsvarsel av 31.mai 2024, s. 11.

³¹ Merknader til forhåndsvarsel av 31.mai 2024, s. 13.

³² Merknader til forhåndsvarsel av 31.mai 2024, s. 13.

Vi understreker forpliktelsen i personvernforordningen artikkel 30 nr. 4 at protokollen skal være klar på etterspørsel fra Datatilsynet. Dette er et sentralt dokument som skal gi oversikt over omfanget av behandlingsaktiviteter i en virksomhet. Dette gjelder uansett om det er behandlingsprotokollen som er gjenstand for tilsyn eller, som i dette tilfelle, om det er andre forhold som undersøkes. Det er derfor ikke tvil om at Telenor ASA ikke bare hadde plikt til å føre behandlingsprotokoll, men at det også hadde plikt til å fremlegge denne for Datatilsynet ved forespørsel.

Vi understreker igjen at plikten til å holde en oppdatert behandlingsprotokoll som oppfyller kravene i artikkel 30 påhviler Telenor ASA som behandlingsansvarlig og databehandler. Vi viser til punkt 13.2.

5.2.3 Om innholdet i behandlingsprotokollen inkludert Telenor ASAs rolle og ansvarsfordeling

Datatilsynet innarbeidet relevante opplysninger i behandlingsprotokollen i foreløpig tilsynsrapport av 11. april 2022. Telenor ASA ga sine merknader til rapporten i brev av 16. mai 2022. Telenor ASAs merknader ble innarbeidet i endelig tilsynsrapport av 30. september 2022. I brev 2. november 2022 ga vi dere mulighet til å komme tilbake med deres mening om hva som bør unntas offentlighet, jf. offentleglova § 13 første ledd og forvaltningsloven § 13 andre ledd punkt 2. I den forbindelse sendte Telenor ASA, i brev av 24. november 2022, nye merknader og vedlegg som runde to til rapporten. Telenor ASAs innspill ble tatt i betraktning i varsel til vedtak som ble sendt til Telenor ASA for kontradiksjon først på engelsk 1. mars 2024 og siden på norsk 18. april 2024. Telenor ASA avga sine merknader til varsel og tilsynsrapport med bilag i brev 31. mai 2024, som inneholdt en del nye påstander og informasjon.

I brevet³³ kommer bl.a. frem:

«Telenor bestrider ikke at oppbygningen av behandlings-protokollen etter omstendighetene kan fremstå som lite tilgjengelig, og være en kime til uklarheter. Det avgjørende er imidlertid hvilke behandlingsaktiviteter som reelt sett finner sted i Telenor ASA.»

Datatilsynet mener Telenor ASA har fått muligheter til å avklare det de anser som aktuelle uklarheter, men ikke minst understreker dette viktigheten av å ha en tilgjengelig, pålitelig og tydelig behandlingsprotokoll på plass som en del av påbudt internkontroll jf. personvernforordningen artikkel 24.³⁴ Den er en del av bevisgrunlaget for tilsynsperioden og skal inneholde faktiske beskrivelser av behandlingsaktivitetene som reelt finner sted. Telenor ASAs påstand om at vi «synes å tillegge Telenor ASA ansvaret for virksomheten som foregår i Telenor Norge AS»³⁵ er ubegrunnet og stemmer ikke. Tilsynets scope er Telenor ASA og

³³ Merknader til forhåndsvarsel av 31.mai 2024, s. 11.

³⁴ Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2019) s. 273 og 275, Eva Jarbekk mfl.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019) s. 257.

³⁵ Merknader til forhåndsvarsel av 31.mai 2024, s. 9.

behandlingsaktivitetene som Telenor ASA står for som behandlingsansvarlig, felles behandlingsansvarlig og/eller databehandler.

Videre hadde Telenor ASA mulighet etter at tilsynet var gjennomført til å foreta opprydding og endringer i protokollen for å gjøre den mer oppdatert hvis dette var nødvendig. Det fremkommer av tilsvaret at selskapet selv var kjent med at protokollen ikke var fullstendig eller i en hensiktsmessig form.³⁶ Selv om dette ikke var tema i tilsynet, hadde og har Telenor ASA en egeninteresse i å sørge for at behandlingsprotokollen oppfyller kravene i artikkel 30. Protokollen utgjør viktig dokumentasjon for både intern og ekstern bruk, og er et dokument som bør oppdateres ved behov. Hensikten med dette er nettopp å sikre at den dokumenterer de reelle behandlingsaktivitetene, slik selskapet selv viser til i tilsvaret. Som Telenor ASA oppgir så har behandlingsprotokollen blitt til ved at ulike personer har fylt ut informasjon:

«Innførlene i protokollen er som nevnt skrevet av ansatte i linjen som kjenner de enkelte aktiviteter godt, men som ikke nødvendigvis har særlig kjennskap til GDPR, eller som for øvrig holder et juridisk presisjonsnivå.»³⁷

Hvis det var kjent at kvaliteten var dårlig ville det vært naturlig at noen fikk ansvar for å følge opp protokollen som helhetlig dokument som et påbudt organisatorisk tiltak etter artikkel 24 nr. 1. Etter artikkel 24 nr. 1 må selskapet iverksette tiltak nettopp for å sikre og påvise at personvernforordningen følges, herunder hva gjelder plikten til å sørge at behandlingsprotokollen er korrekt og oppdatert til enhver tid etter artikkel 30.³⁸ Dette er også et arbeid som personvernombudet kunne blitt involvert i, jf. personvernforordningen artikkel 38 nr. 1. Behandlingsprotokollen utgjør også et viktig verktøy for personvernombudet slik at vedkommende har mulighet til å ha oversikt over hvilke behandlingsaktiviteter virksomheten utfører, og dermed også vurdere hvilke områder vedkommende bør involvere seg i.

Telenor ASA sier i tilsvaret at behandlingsprotokollen ikke gir uttrykk for de reelle behandlingsaktivitetene. Dette har de ved flere anledninger hatt mulighet til å uttale seg om til Datatilsynet. Vi fastholder at Telenor ASA har fått anledning til kontradiksjon underveis i sakens forløp, også på dette punktet. Telenor ASA har forelagt noe ny informasjon i tilsvaret som utfyller den vi har fått tidligere.

Det fremkommer i Telenor ASA sin behandlingsprotokoll at Telenor ASA behandler personopplysninger om egne ansatte (nåværende, tidligere og potensielt fremtidige), pårørende og familiemedlemmer til ansatte, kunder i Telenor Group, leverandører, andre kontraktspartnere, konsulenter, innleide ressurser, besøkende (fysisk og digitalt), styremedlemmer, medlemmer av Corporate Assembly, og nomination committee.³⁹

³⁶ Merknader til forhåndsvarsel av 31.mai 2024, s. 13.

³⁷ Merknader til forhåndsvarsel av 31.mai 2024, s. 14.

³⁸ Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad & Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2019) s. 273 og 304, Eva Jarbekk et al.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019) s. 257 og 280.

³⁹ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

Videre kommer frem i behandlingsprotokollen at Telenor ASA også behandler personopplysninger fra andre datterselskaper i Telenor Group, se også punkt 3.3.2 i den endelige tilsynsrapporten.⁴⁰ Dette gjelder først og fremst personopplysninger om ansatte i Telenor Group (antall ca. 15 000⁴¹), men også i begrenset grad om kunder.⁴²

Telenor ASA beskriver i protokollen at de er behandlingsansvarlig for mange behandlingsaktiviteter som dekker blant annet intern varsling, granskning, spørreundersøkelser, lydopptak av møter, evalueringer, utvikling av talenter, avviksmeldinger m.m. fra følgende enheter: Group Internal Audit & Investigation, Group Legal, Group People & Sustainability og Group Strategy & Ext. Relations,⁴³

I to tilfeller skriver Telenor ASA at de er felles behandlingsansvarlig. Telenor ASA presiserer i sine merknader til forhåndsvarsel⁴⁴ at «i svært liten utstrekning har forekommet eller forekommer tilfeller av felles behandlingsansvar i konsernet» og at dere mener det «er feil når tilsynet for eksempel synes å anta at det foreligger felles behandlingsansvar i nevneverdig utstrekning.» Datatilsynet mener at det som er viktigere i denne sammenheng enn antall behandlingsaktiviteter er blant annet art og omfang inkludert antall registrerte og/eller formål som krever regelmessig og systematisk monitorering i stor skala jf. personvernforordningen artikkel 37 nr. 1 bokstav b.

Den ene behandlingsaktiviteten er for HR-informasjon behandlet i systemet [REDACTED] av Group People & Sustainability for alle ansatte i konsernet (ca. 15 000). Telenor ASA forklarer:

«[REDACTED] is Telenor's core HRIS maintaining an overview of all of our employees and the organizational structure. [REDACTED] contains employees personal information, job/role and employment related details, compensation and benefits overview, career profile details and talent related data.»⁴⁵

Telenor ASA nevner i sine merknader til varsel at de:

«trolig i noe større utstrekning under den perioden tilsynet gjelder enn i dag, hadde en IT-administratorrolle for verktøyene som Telenor-konsernet bruker, for å håndtere ansattopplysninger [REDACTED] samt legge til rette for informasjon til og samhandling mellom ansatte [REDACTED]. Også i tilsynsperioden var det rettslig sett klart at det var det enkelte selskapet i Telenor konsernet som benyttet systemet som var behandlingsansvarlig for sin egen bruk.»⁴⁶

⁴⁰ Endelig tilsynsrapport av 30. september 2022, s. 5-10.

⁴¹ Endelig tilsynsrapport av 30. september 2022, s. 11.

⁴² Telenor ASAs artikkel 30-protokoll av 2. februar 2022, Endelig tilsynsrapport av 30. september 2022, s. 5-6.

⁴³ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

⁴⁴ Merknader til forhåndsvarsel av 31. mai 2024, s. 13.

⁴⁵ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

⁴⁶ Merknader til forhåndsvarsel av 31. mai 2024, s. 12.

Det er behandlingsaktivitetene i tilsynsperioden som ligger til grunn i vedtaket. Ifølge behandlingsprotokollen beskriver Telenor ASA at de for [REDACTED] behandlingsaktiviteten er felles behandlingsansvarlig. Det faktum at det enkelte selskapet i Telenor konsernet også har behandlingsansvar reduserer ikke på noe vis ansvaret som hviler på Telenor ASA som felles behandlingsansvarlig. Det er ikke slik at felles behandlingsansvarlige nødvendigvis har like stort ansvar.⁴⁷ Datatilsynet bemerker at Telenor ASA selv opplyser at under tilsynsperioden behandlet de ansattopplysninger for hele konsernet, både som felles behandlingsansvarlig og databehandler.⁴⁸

Den andre behandlingsaktiviteten som Telenor ASA beskriver at selskapet er felles behandlingsansvarlig for, gjaldt [REDACTED], som ifølge protokollen var satt på pause men skulle starte på nytt i første kvartal 2022. Det kommer fram at de registrerte er kunder og at antallet er anslått til [REDACTED]. Behandlingen beskrives av Telenor ASA: «Processing of aggregated market research data (customers and non-customers) to produce charts, overviews, summary tables - and executive level reporting.»⁴⁹

I tillegg beskriver Telenor ASA i behandlingsprotokollen at de er databehandlere for flere forskjellige behandlingsaktiviteter. Group Internal Audit & Investigations behandler internrevisjoner som berører nåværende og tidligere ansatte, konsulenter, leverandører og kunder, og antall registrerte er oppgitt til [REDACTED].

Telenor Research under Group Strategy & Ext. Relations opptrer som databehandler for bl.a. følgende:⁵⁰

Multi-country, multi-year surveys in Telenor's markets to understand customer behaviours.	Customers
The purpose of the processing activity is to train machine learning algorithms on audio- and transcription data for speech recognition. The data comes from Telenor Norway.	Current Employees; #Customers
Statistical analysis and machine learning of chatbot datasets from and on behalf of Telenor Norway (data controller).	Customers

Kategorier av personopplysninger som blir listet er:

“Behavior;#Demographics;#Ownership and possessions;#Electronic devices and usage;#Communication;#Preferences or interests;#Contact details;#Family, Family;#Communication;#Electronic devices and usage;#Contact

⁴⁷ Se for eksempel saker C-210/16, *Wirtschaftsakademie*, EU:C:2018:388, avsnitt 43; C-2517 *Jehovas vitner*, ECLI:EU:C:2018:551, avsnitt 66.

⁴⁸ Merknader til forhåndsvarsel av 31. mai. 2024, s. 12.

⁴⁹ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

⁵⁰ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

details;#Location;#Identification;#Life history and events;#Behavior;#Preferences or interests;#Location”⁵¹

Antall registrerte i behandlinger med Telenor ASA som databehandler er opplyst at løper fra 100-250 som laveste og til 25K-100K som høyeste antall.⁵²

I vår tilsynsrapport har vi skrevet på sider 8-10:

«Tidligere personvernombud i Telenor ASA har i flere omganger påpekt uavklarte forhold med tanke på behandlingsansvar. I PowerPoint-presentasjon lagt frem på i GU Forum 9. september 2021 ble blant annet følgende risikoer fremhevet:

“Internal data sharing governance - Personal data is shared between business units within Telenor without adequate data sharing governance, including legal transfer mechanisms, clear definition of controller/processor relationships, and generally diffusion of responsibility.”⁵³

- “Lack of transparency into existing agreement setups [+I/P]
- Often symptoms showing of unclear division of responsibility [+I/P]
- Lack of knowledge re. differing legal requirements in TN-regions [+I/P]
- Differing opinions and non-standardization of roles and terms for business initiative governance [+P]”⁵⁴

Til beskrivelsen ovenfor har Telenor ASA kommentert at den er misvisende fordi bekymringene vedrørte den behandlingen Telenor ASA i hovedsak utfører, altså behandling av ansattopplysninger. Videre hevder Telenor ASA at det ikke er noen uklarhet når det gjelder behandling av kundedata, «som i hovedsak gjøres av de ulike datterselskapene til Telenor ASA som telekom-operatører, og hvor Telenor ASAs eventuelle rolle i behandlingen av dette primært er som databehandler gjennom Telenor Research og GIAI».⁵⁵

Datatilsynet har ikke grunnlag for å fastslå at uttalelsen fra det eksterne personvernombudet gjelder kundedata, men ser ikke hvordan beskrivelsen bare kan angå ansattopplysninger i Telenor ASA. Bekymringen gjelder deling av personopplysninger mellom «Business Units» i Telenor-gruppen. Telenor ASA har ikke lagt frem argumenter eller dokumentasjon som underbygger påstanden om at den generelle beskrivelsen over gjelder ansattopplysninger. Uavhengig av hvilke personopplysninger det er tale om, fremstår det slik at ansvarsforholdene har vært uavklarte.

Videre har det eksterne personvernombudet uttrykt følgende i en e-postkorrespondanse i kontekst av Schrems II-problematikk, som viser bekymring med hensyn til fordeling av behandlingsansvar på et generelt plan:

⁵¹ Telenor ASAs artikkel 30-protokoll av 2. februar 2022

⁵² Telenor ASAs artikkel 30-protokoll av 2. februar 2022

⁵³ «2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf», s. 13.

⁵⁴ «2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf», s. 14.

⁵⁵ Foreløpig tilsynsrapport – med kommentarer fra Telenor ASA i gult, 16.5.2022, s. 8.

- «In my opinion, for initiatives rolled out by, or directed by ASA, ASA should be regarded a “data controller” under the law and through that will have several obligations to adhere to which cannot simply be outsourced. That is not to say that some concrete activities may not be outsourced, but privacy accountability cannot, and consequently a not insignificant level of involvement by ASA business-, system- and contract owners will be required regardless of outsourcing. Put differently, as long as ASA has an operational involvement in business activities involving processing of personal data, whether it’s within ASA itself or exercised upon other businesses through ASAs role as HQ, there are privacy obligations to adhere to that ASA cannot fully escape. With that said, I am of course looking forward to Group Legal’s assessment on this topic!
- Currently, there seems to be a dilution of responsibility between the entities mentioned, where no single party takes full responsibility of privacy issues/activities or is even capable of doing it. For example:
 - BUs may be struggling with the conundrum of being “accountable for their own privacy”, while at the same time being required to adopt what comes down the pipe from ASA/GSS/TPC and themselves being unable to impact product/system features, contracts or even privacy assessments – and expecting that things they are directed to do business wise has been properly checked out privacy wise, which is often not the case;
 - GSS may be expected to implement systems and features as prescribed by a business owner at ASA, even potentially impacting data flows or data access of other BUs or between ASA/BUs, but where GSS is lacking ownership, involvement or access to assessments or contracts/frameworks enabling this;
 - TPC may be entering into contracts under their mandate, which then typically has a commercial focus and an inadequate privacy focus, impacting all later (privacy) activity down the chain;
 - ASA does not have (my opinion) the proper awareness, competence and/or resources to do necessary compliance work with sufficient quality and timeliness (including catching up with backlog), on behalf of itself or group initiatives that other BUs must rely upon. There are simply things falling through the cracks with how things are currently set up.»⁵⁶

Telenor ASA har påpekt at det første avsnittet i sitatet spesifikt gjelder en potensiell outsourcing av enkelte operasjonelle personvernrelaterte arbeidsoppgaver i Telenor ASA til Telenor Global Shared Services (GSS), som per dags dato ikke har blitt gjennomført. Telenor ASA mener derfor det første avsnittet ikke er relevant for tilsynet, og at disse generelle

⁵⁶ Fra e-postkorrespondanse «Mail to EVP People», 13.04.2021».

bekymringene har blitt fulgt opp i dialog mellom personvernombudet og ledelsen.⁵⁷ Selv om e-posten er sendt i den konteksten, er det nødvendig å se på ordlyden. Formuleringen han bruker er «for initiatives rolled out by, or directed by ASA». Datatilsynet finner derfor uttalelsen relevant, da den viser en bekymring med hensyn til forståelse av ansvarsfordeling for ulike behandlingsaktiviteter, selv om den konkrete outsourcingen ikke ble gjennomført.

Telenor ASA mener vår omtale i tilsynsrapporten om Telenor ASAs behandling av kundedata ikke er dekkende for de faktiske behandlingsaktivitetene.⁵⁸ Vi har skrevet rapporten og forhåndsvarsel til vedtak basert på innleverte dokumenter inkludert oppgitte opplysninger i behandlingsprotokollen og intervjuer. Dersom beskrivelsene likevel ikke er dekkende har det sammenheng med at informasjon tidligere mottatt fra selskapet har vært mangelfull eller uriktig. Vi registrerer at det er først da saken ble satt på spissen med varsel om vedtak at vi fikk mer detaljert informasjon i tilsvaret fra selskapet.

Telenor påstår i sine merknader til forhåndsvarsel at Telenor ASA ikke behandler store mengder kundedata og/eller personopplysninger av mer inngripende karakter som databehandler til tross for at vår oppfatning er basert på beskrivelsene i deres behandlingsprotokoll.

Telenor ASA skriver i sine merknader til forhåndsvarsel:

«I dette systemet er det visse standardiserte og til dels forhåndsutfylte tekstbokser og emneknagger som den som fyller inn protokollen velger mellom, noe som i visse tilfeller kan lede til at innholdet i protokollen kan misforstås/bli fylt ut feil, for eksempel i angivelsen av hvem som er de registrerte, antallet registrerte, hvilke typer av personopplysninger som behandles osv. I ettertid ser Telenor at det er slike kilder til misforståelser og feil i det dokumentet som er oversendt Datatilsynet. For eksempel ser selskapet at det på en rekke punkter er angitt tall som kan etterlate et inntrykk av en behandling av personopplysninger i større skala og omfang enn hva som er tilfellet. Ut fra angivelsen av hvilke typer av opplysninger som behandles, er det enkelte steder lett å misforstå hva behandlingen egentlig går ut på, og hvilken informasjon det egentlig er snakk om. Det er også andre sider ved selve oppsettet i løsningen som benyttes, som selskapet ser har påvirket innholdet i det oversendte på en måte som kan lede til feilslutninger eller misforståelser. Det er derfor uheldig at Datatilsynet har lagt til grunn en bokstavtolkning av innholdet, uten å ta høyde for Telenors forsøk på å forklare de faktiske forholdene som ligger til grunn for uttrekket.»⁵⁹

Som nevnt over er det Telenor ASAs ansvar, som behandlingsansvarlig og databehandler, å sørge for at behandlingsprotokollen er utfylt og oppdatert. Dette inkluderer at informasjonen er korrekt. Selskapet må regne med at Datatilsynet støtter seg til og legger til grunn innholdet i innlevert behandlingsprotokoll. Dette er selve formålet med en behandlingskontroll, jf. personvernforordningen fortalespunkt 82:

⁵⁷ Foreløpig tilsynsrapport – med kommentarer fra Telenor ASA i gult, 16.5.2022, s. 9.

⁵⁸ Merknader til forhåndsvarsel av 31.mai 2024, s. 16-17.

⁵⁹ Merknader til forhåndsvarsel av 31. mai 2024, s. 13.

«For å påvise samsvar med denne forordning bør den behandlingsansvarlige eller databehandleren føre protokoll over de behandlingsaktiviteter som de har ansvar for. Hver behandlingsansvarlig og hver databehandler bør ha plikt til å samarbeide med tilsynsmyndigheten og på anmodning gjøre disse protokollene tilgjengelig for den, slik at de kan benyttes til tilsyn med nevnte behandlingsaktiviteter.»

Dersom selskapet selv mener at behandlingsprotokollen var, og fortsatt er, misvisende, så ligger det innenfor plikten etter artikkel 30, supplert med artikkel 24, å sørge for at behandlingsprotokollen blir korrigert og revidert. Hvis det er mangler ved innholdet fordi ulike personer har manglet kompetanse til utfylling eller løsningen som blir brukt ikke er egnet, er dette forhold som Telenor ASA burde sørget for at det forelå rutiner, oppfølging eller andre egnede organisatoriske og tekniske tiltak for å sikre at protokollen er så oppdatert og korrekt som mulig. Dersom det foreligger informasjon i andre mer egnede systemer, forventer vi at dette ville blitt oversendt med tilsvaret.

Vi registrerer at det i tilsvaret gis mer utfyllende informasjon. Dette er nyttig, men etter vår vurdering viser dette at behandlingsaktivitetene som blir omtalt har et betydelig omfang og at Telenor ASAs behandlingsaktiviteter ikke er begrenset til kun enkel HR-administrasjon for ansatte i Telenor ASA. Denne informasjonen bekrefter igjen at selskapet også opptrer som felles behandlingsansvarlig og som databehandler, og ikke bare som behandlingsansvarlig. Dette må inngå i vurderingen av blant annet om selskapet er forpliktet å ha personvernombud eller ikke. Det kommer også frem i tilsvaret at Telenor ASA behandler kundedata i noen grad når de skriver: «det *i alt det vesentlige* er mobilselskapene i Telenor-konsernet som behandler opplysninger relatert til eksterne kunder, og ikke Telenor ASA.»⁶⁰ (vår kursiv).

Vi minner også om at hvorvidt en virksomhet har rolle som behandlingsansvarlig, felles behandlingsansvarlig og/eller databehandler beror på de faktiske forholdene og ikke formelle roller.⁶¹ Uavhengig av hvilken konsernstruktur Telenor har valgt og hvilken rolle som er definert for Telenor ASA, er det de faktiske forholdene i selskapet og dets relasjon til datterselskapene som skal legges til grunn.

5.2.4 Angående kontaktopplysninger

På tilsynsdagen kunne vi ikke finne kontaktopplysningene til Telenor ASAs personvernombud på Telenors nettsider. Telenor ASA forklarte at kontaktopplysningene var tilgjengelig på intranett for de ansatte siden behandlingen av personopplysninger for det meste gjelder ansatte og interne relasjoner.⁶² Dette har ikke blitt bekreftet, men vi legger til grunn at de ansatte kjente til hvem personvernombudet i Telenor ASA var og hvordan de kunne komme i kontakt med vedkommende.

⁶⁰ Merknader til forhåndsvarsel av 31.mai 2024, s. 10.

⁶¹ Se for eksempel EU-domstolen sak C-638/21 *NVSC* ECLI:EU:C:2023:949 avsnitt 29-31. Se også EDPB Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse Version 2.0 vedtatt 7. juli 2021 avsnitt 12 «Begreberne dataansvarlig og databehandler er funksjonelle begreber: De har til formål at fordele ansvaret etter parternes egentlige roller.»

⁶² Foreløpig tilsynsrapport – med kommentarer fra Telenor ASA i gult, 16.5.2022, s. 3.

Datatilsynet bemerker at det er av avgjørende at *alle* registrerte, interne og eksterne, har enkel tilgang til kontaktopplysningene til selskapets personvernombud, uavhengig av om selskapet opptrer som behandlingsansvarlig eller databehandler. Vi anser dette som en forutsetning for å kunne sikre de registrertes rettighet i henhold til personvernforordningen artikkel 38 nr. 4. Kontaktinformasjonen til personvernombudet bør derfor offentliggjøres for eksempel på selskapets nettsted, og det bør gjøres klart at det faktisk er personvernombudet som er mottaker til e-post adressen. For eksempel vil en generisk e-postadresse til kundeservice etter vår mening ikke være tilfredsstillende.

Vår vurdering er at dette utgjør en delvis overtredelse av personvernforordningen artikkel 37 nr. 7, men finner for øvrig at Telenor ASA overholder artikkel 37, innenfor tilsynets ramme. Vi bemerker at Telenor ASA oppdaterte personvernerklæringen på nett 3. februar 2022 med kontaktopplysninger til personvernombudet.⁶³

5.2.5 Konklusjon

Tilsynet har avdekket en uoversiktlig og ufullstendig behandlingsprotokoll hos Telenor ASA og uklarheter rundt bl.a. Telenor ASAs ansvar for bestemte behandlingsaktiviteter, kategorier av personopplysninger og antall registrerte som må ryddes opp i. Behandlingsprotokollen skal leveres Datatilsynet på forespørsel jf. personvernforordningen artikkel 30 nr. 4 og fortalepunkt 82. Dermed må virksomheten være bevisst på viktigheten av å vedlikeholde protokollen og at denne kan og vil bli lagt til grunn som bevis ved tilsyn.

Basert på Telenor ASAs behandlingsaktiviteter, som beskrevet ovenfor, mener vi det ikke er åpenbart at selskapet ikke skal ha et personvernombud. Dette må ses i sammenheng med hvilke roller selskapet har som henholdsvis behandlingsansvarlig, felles behandlingsansvarlig og databehandler. Deretter hva disse aktivitetene faktisk går ut på. Telenor ASA må derfor vurdere hvorvidt de har plikt eller ikke til å ha personvernombud og dokumentere denne vurderingen før det kan konkluderes.

6 Involvering av personvernombud, personvernforordningen artikkel 38 nr. 1

6.1 Tilsynskriterier og tilsynsbevis

Personvernforordningen artikkel 38 nr. 1 lyder som følger:

«Den behandlingsansvarlige og databehandleren skal sikre at personvernombudet på riktig måte og i rett tid involveres i alle spørsmål som gjelder vern av personopplysninger.»

Videre har den behandlingsansvarlige i forbindelse med utførelsen av en vurdering av personvernkonsekvenser (Data Protection Impact Assessment (DPIA)) plikt til å rådføre seg med personvernombudet etter personvernforordningen artikkel 35 nr. 2. Vi viser videre til punkt 3.2.1 og 3.2.2 i den endelige tilsynsrapporten av 30. september 2022.

⁶³ <http://www.telenor.com/privacy-policy/>

6.2 Datatilsynets vurdering

I henhold til ordlyden i personvernforordningen artikkel 38 nr. 1 skal personvernombudet involveres «på riktig måte» og «i rett tid» i alle spørsmål som gjelder vern av personopplysninger. Disse kravene krever en forholdsmessighetsvurdering, ettersom hva som anses som «riktig måte» og «i rett tid», vil variere avhengig av spørsmålenes kompleksitet og art. Dette krever at behandlingsansvarlig har etablert egnede tiltak slik som interne rutiner, for å sikre at involveringen av personvernombudet oppfyller kravene i personvernforordningen artikkel 38 nr. 1. Uten noen form for intern, dokumentert standardprosedyre vil det være vanskelig for de ansatte å vurdere hva som anses som «riktig måte» og «i rett tid» i hvert enkelt tilfelle.

Den tidligere Artikkel 29-gruppens (Article 29 Data Protection Working Party) veiledning om personvernombud, som ble tilsluttet av Personvernrådet (European Data Protection Board (EDPB)), gir eksempler på hva virksomheter kan gjøre for å overholde bestemmelsen:

«[...]organisationen [bør] for eksempel sikre, at:

- databeskyttelsesrådgiveren regelmessigt inviteres til at deltage i møder på senior- og mellemliderniveau
- databeskyttelsesrådgiverens tilstedeværelse er ønskværdig, når der skal tages beslutninger, som har en databeskyttelsesdimension. Alle relevante oplysninger skal videregives rettidigt til databeskyttelsesrådgiveren, så denne kan give passende rådgivning
- databeskyttelsesrådgiverens udtalelser altid tillægges behørig vægt. I tilfælde af uenighed anbefaler Artikel 29-gruppen som god praksis at dokumentere årsagerne til, at databeskyttelsesrådgiverens henstillinger ikke følges.
- databeskyttelsesrådgiveren omgående høres i tilfælde af, at et brud på datasikkerheden eller en anden hændelse har fundet sted.

Når det er relevant kan den dataansvarlige eller databehandleren udvikle retningslinjer eller programmer for databeskyttelse som fastlægger, hvornår databeskyttelsesrådgiveren skal høres.»⁶⁴

Personvernrådets retningslinjer er ikke bindende, men fastsetter momenter som vil være relevante i vurderingen av om en virksomhet overholder personvernforordningen artikkel 38 nr. 1. Personvernrådets retningslinjer gjenspeiler den felles forståelsen og praksisen til tilsynsmyndighetene for personvern i EØS. De er derfor en relevant kilde for å tolke personvernforordningen, særlig med tanke på å sikre en ensartet anvendelse av personvernforordningen i hele EØS, slik det kreves i personvernforordningen artikkel 51 nr. 2 og artikkel 70 nr. 1.⁶⁵

⁶⁴ WP 243 rev.01 «Retningslinjer for databeskyttelsesrådgivere», s. 14.

⁶⁵ Se personvernforordningen fortalepunkter 10, 123 og 139.

Telenor Groups retningslinjer for personvern (Group Privacy Policy) fastsetter at hvert selskap i konsernet (Business Unit/forretningsenhet):

«shall appoint a Data Protection Officer who advises and reports on privacy matters to the top level of management in the Business Unit [...]»⁶⁶

Telenor Groups personvernhandbok (Group Manual Privacy) fastsetter at personvernombudet skal:

«[a]dvice management and personnel in the Business Unit on risks and best practices related to processing of personal data, including the resources needed and effort required in order to manage privacy risk in the processing activities of the Business Unit and the privacy impact of processing activities».⁶⁷

Disse to interne dokumentene fastsetter overordnede forpliktelser for alle selskaper i konsernet, herunder Telenor ASA.

I henhold til konsernets personvernhandbok skal vurderinger av personvernkonsekvenser («Data Protection Impact Assessment» (DPIA)) som et minimum:

«[i]nclude an independent recommendation from the DPO before the assessment is concluded».⁶⁸

Videre bør personvernombudet i tilfelle personvernshendelser som et minimum:

«be consulted for his/her independent opinion on assessments of the breach impact and the risk it poses to the individuals, as well as the effect of mitigating controls in limiting the incident».⁶⁹

Ut over det som følger av ovennevnte generelle interne krav til alle selskaper i Telenor Group, ble Datatilsynet under tilsynet ikke forelagt noen skriftlige rutiner eller andre særlige retningslinjer for Telenor ASA angående når og på hvilken måte Telenor ASAs personvernombud skal involveres i spørsmål som gjelder vern av personopplysninger.

Den eneste interne standardprosessen for involvering av personvernombudet vi har identifisert under tilsynet, består av regelmessige møter mellom personvernombudet og funksjoner i linjeorganisasjonen, dvs. gjennom «Group Unit Forum (GU Forum)» og møter med personvernkoordinatorer («Privacy Coordinators») i linjeorganisasjonen. Disse regelmessige møtene er imidlertid et resultat av den senere utviklingen, som beskrevet under.

⁶⁶ «Group Privacy Policy, valid from: 2022-01-01», s. 1.

⁶⁷ «Group Privacy Manual, valid from: 2022-01-01» s. 1.

⁶⁸ «Group Privacy Manual, valid from: 2022-01-01» s. 6.

⁶⁹ «Group Privacy Manual, valid from: 2022-01-01» s. 8.

Telenor ASAs personvernombud begynte å delta på møter i GU Forum i september 2021.⁷⁰ Mens involvering av personvernombudet krever at linjeorganisasjonen tar kontakt med personvernombudet for råd om spørsmål som oppstår, var hovedhensikten med ombudets deltakelse i GU Forum å etablere en fungerende rapporteringslinje for personvernombudet:

«... [the CEO] agreed that it would be useful to delegate the authority of privacy reporting from the DPO in Telenor ASA, from [the CEO], to the Policy owner and Group Unit forum».⁷¹

Før personvernombudet begynte å delta på møter i GU Forum, kunne vedkommende delta på «Compliance Committee Meetings» (CCM), men ombudet deltok ikke regelmessig på disse møtene. Møtene var i mindre grad egnet for involvering av personvernombudet, siden møtene var avgrenset til håndtering av spørsmål i Telenor Group og ikke særlig viet personvernspørsmål, se punkt 3.5.2 i den endelige tilsynsrapporten av 30. september 2022.

Personvernkoordinatorerne i de ulike enhetene i Telenor ASAs linjeorganisasjon har ukentlige møter med personvernombudet der de kan drøfte personvernspørsmål.⁷² Det eksterne personvernombudet⁷³ nevnte i intervjuet at det hadde vært avgjørende å få på plass personvernkoordinatorer i alle konsernenhetene. Han uttalte videre at før utnevnelsen av disse koordinatorerne hadde ikke personvernombudet tilstrekkelige koblinger til alle de ulike delene av selskapet.⁷⁴

Telenor ASA har uttalt at personvernombudet har regelmessige møter med Group Legal og den midlertidig innleide Schrems II-ressursen, og at det i disse møtene er mulig å utveksle informasjon.⁷⁵ Datatilsynet har ikke blitt forelagt dokumenter som formaliserer forekomsten av slike regelmessige møter.

Ut over ovennevnte møter blir Telenor ASAs personvernombud involvert i spørsmål som gjelder vern av personopplysninger, fra sak til sak.⁷⁶ Slik var det også før disse regelmessige møtene ble etablert. Den endelige tilsynsrapporten beskriver hvordan involveringen foregår i det enkelte tilfelle.⁷⁷ Tilsynelatende foregikk det en viss ad hoc-involvering av personvernombudet i personvernspørsmål mellom oktober 2020 og januar 2022. Ettersom denne involveringen var såpass uformell, er det imidlertid vanskelig for Datatilsynet å vurdere i hvilken grad Telenor ASAs personvernombud har vært involvert i «alle spørsmål som gjelder vern av personopplysninger», jf. personvernforordningen artikkel 38 nr. 1.

Selv om vi anser at det har vært en risiko for at Telenor ASAs personvernombud ikke har vært involvert på «riktig måte» og i «rett tid» i alle spørsmål som gjelder vern av

⁷⁰ Endelig tilsynsrapport av 30. september 2022, s. 20.

⁷¹ E-post der konsernsjefen (CEO) delegerer ansvaret for personvernombudets rapportering.

⁷² Intervju med personvernombudet i Telenor ASA, og personvernkoordinatorer.

⁷³ «Det eksterne personvernombudet» refererer til ombudet som var innleid fra [redacted] i perioden januar 2021 til oktober 2021 jf. endelig tilsynsrapport av 30. september, s. 2.

⁷⁴ Endelig tilsynsrapport av 30. september 2022, s. 13.

⁷⁵ Endelig tilsynsrapport av 30. september 2022, s. 3.

⁷⁶ «Response to Datatilsynet», 13.12.2021 s. 8.

⁷⁷ Endelig tilsynsrapport av 30. september 2022, s. 3–4.

personopplysninger, konkluderer vi ikke med overtredelse av personvernforordningen artikkel 38 nr. 1 innenfor tilsynsperioden, da det ikke foreligger sannsynlighetsovervekt. Vi finner en mangel på retningslinjer som sørger for klargjøring i hvilke tilfeller og på hvilken måte personvernombudet bør involveres. Se punkt 12.2 om de rettslige kravene i personvernforordningen artikkel 24 nr. 1 og 2 om å innføre organisatoriske tiltak og egnede retningslinjer for vern av personopplysninger, som har et tilstrekkelig og tydelig innhold.

7 Tildeling av ressurser, personvernforordningen artikkel 38 nr. 2

7.1 Tilsynskriterier og tilsynsbevis

Personvernforordningen artikkel 38 nr. 2 lyder som følger:

«Den behandlingsansvarlige og databehandleren skal støtte personvernombudet i forbindelse med utførelsen av oppgavene nevnt i artikkel 39 ved å stille til rådighet de ressurser som er nødvendig for å utføre nevnte oppgaver, samt gi tilgang til personopplysninger og behandlingsaktiviteter og gjøre det mulig for vedkommende å opprettholde sin dybdekunnskap.»

Vi viser videre til punkt 3.3.1 og 3.3.2 i den endelige tilsynsrapporten av 30. september 2022.

Personvernforordningen artikkel 39 nr. 2 fastsetter følgende:

«Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i.»

Vi viser til punkt 3.8 i den endelige tilsynsrapporten om personvernombudets oppgaver nevnt i artikkel 39.

7.2 Datatilsynets vurdering

Kravet om å stille nødvendige ressurser til rådighet for at personvernombudet skal kunne utføre sine oppgaver er et generelt, overordnet krav. I tillegg spesifiserer personvernforordningen artikkel 38 nr. 2 en plikt til å gi personvernombudet tilgang til personopplysninger og behandlingsaktiviteter, og gjøre det mulig for vedkommende å opprettholde sin dybdekunnskap.

I henhold til artikkel 39 har personvernombudet som oppgave å informere og gi råd til den behandlingsansvarlige eller databehandler, og kontrollere overholdelse av den behandlingsansvarliges eller databehandlerens ansvar. En tydeliggjøring av Telenor ASAs rolle er derfor viktig i vurderingen av om personvernombudet er tildelt tilstrekkelige ressurser til å utføre sine oppgaver.

Den tidligere Artikkel 29-arbeidsgruppens veiledning om personvernombud gir retningslinjer for hva som bør gjøres for å oppfylle kravene i personvernforordningen artikkel 38 nr. 2:

«Navnlig skal følgende punkter tages i betragtning:

- Aktiv støtte til databeskyttelsesrådgiverens funktion fra seniorledelsen (såsom på bestyrelsesniveau).
- Tilstrækkelig tid til databeskyttelsesrådgiverne til at gennemføre deres opgaver. Dette er især vigtigt, hvor en intern databeskyttelsesrådgiver udpeges på deltidsbasis, eller hvor den eksterne databeskyttelsesrådgiver udfører databeskyttelse i tilslutning til andre opgaver. Ellers vil modstridende prioriteter kunne resultere i, at databeskyttelsesrådgiverens pligter forsømmes. Det er altafgørende, at der er tilstrækkelig tid til databeskyttelsesrådgiverens opgaver. Det er god praksis at afsætte en procentdel af tiden til databeskyttelsesrådgiverfunktionen, når den ikke udføres på heltidsbasis. Det er også god praksis at bestemme tiden, som er nødvendig til at udføre funktionen, det passende prioritetsniveau for databeskyttelsesrådgiverens pligter og at databeskyttelsesrådgiveren (eller organisationen) udarbejder en arbejdsplan.
- Passende støtte i form af finansielle ressourcer, infrastruktur (lokaler, faciliteter, udstyr) og eventuelt personale.
- Officiel kommunikation af udpegelsen af databeskyttelsesrådgiveren til alt personale for at sikre, at dennes eksistens og funktion er kendt inden for organisationen.
- Nødvendig adgang til andre afdelinger som personale, juridisk, IT, sikkerhed osv., så databeskyttelsesrådgiverne kan modtage afgørende støtte, input og oplysninger fra disse andre afdelinger.
- Løbende efter- og videreuddannelse. Datasikkerhedsrådgivere skal have mulighed for at holde sig ajour med hensyn til udviklingen inden for databeskyttelse. Målet bør være konstant at øge datasikkerhedsrådgivernes ekspertiseniveau, og de bør tilskyndes til at deltage i kurser om databeskyttelse og andre former for professionel udvikling, såsom at deltage i fora for privatlivets fred, workshops osv.
- Afhængigt af organisationens størrelse og struktur kan det være nødvendigt at oprette et databeskyttelsesrådgivningsteam (en databeskyttelsesrådgiver og dennes personale). I sådanne tilfælde skal teamets interne struktur samt opgaver og ansvar for hvert enkelt medlem være tydeligt fastsat. Tilsvarende, når databeskyttelsesrådgiverens funktion udøves af en ekstern tjenesteyder, kan et team af personer, som arbejder for denne enhed, effektivt udføre databeskyttelsesrådgiverens funktioner som team under en persons ansvar, der er udpeget som overordnet kontakt for kunden.

Generelt forholder det sig således, at jo mere komplekse og/eller følsomme behandlingsprocesserne er, jo flere ressourcer skal databeskyttelsesrådgiveren tildeles. Databeskyttelsesfunktionen skal være effektiv og tilstrækkeligt veludstyret med ressourcer i forhold til den databehandling, som udføres.»⁷⁸

⁷⁸ WP 243 rev.01 «Retningslinjer for databeskyttelsesrådgivere» vedtatt 13. desember 2016, s.15.

Selv om veiledningen ikke er bindende, legger den frem momenter som er relevante i vurderingen av om en organisasjon overholder kravene i personvernforordningen artikkel 38 nr. 2.

Vi viser videre til den endelige tilsynsrapporten av 30. september 2022, s. 10–11, for den faktiske bakgrunnen.

Tilstrekkelig tid til at personvernombudet kan utføre sine oppgaver

Å sette av tilstrekkelig tid til at personvernombudet kan utføre sine oppgaver er et av hovedmomentene for å sikre overholdelse av personvernforordningen artikkel 38 nr. 2.

Telenor ASAs personvernombud⁷⁹ er utnevnt i 50 prosent stilling, mens de resterende 50 prosentene av årsverket i prinsippet skal brukes som advokatfullmektig i Telenor ASAs Group Legal-avdeling.⁸⁰ Telenor ASA presiserer at personvernombudet siden oktober 2020 i praksis har brukt mesteparten av arbeidstiden sin på oppgaver knyttet til rollen som personvernombud.⁸¹ Dette var imidlertid ikke formalisert i noe dokument Telenor ASA forela for Datatilsynet. Flere ulike personer har ved flere anledninger påpekt at et årsverk på 50 prosent til å ta seg av personvernombudets oppgaver verken er eller har vært tilstrekkelig i praksis.⁸²

Videre tyder flere omstendigheter på at heller ikke den nevnte økningen av tiden som blir brukt på personvernombudets oppgaver, har vært tilstrekkelig. Basert på dokumentasjonen vi mottok, var det et stort etterslep i første halvdel av 2021,⁸³ noe som også tyder på at personvernombudet ikke hadde nok tid til å utføre oppgavene sine. I den forbindelse bemerket det eksterne personvernombudet i september 2021 at «DPO spends 50 % more time than originally intended, while still being overburdened with tasks and being a bottleneck», og at «[m]ost time [is] spent on retro-active issue management, instead of pro-active and strategic work». ⁸⁴ Dette tyder på mangel på ressurser når det gjelder personvernombudets evne til å utføre sine oppgaver.

Telenor ASAs ledelse opplyste at de ville undersøke om det er behov for formelt å tildele et 100 prosent årsverk til Telenors personvernombud.⁸⁵ Vi anser at et årsverk på 50 prosent med en fleksibel, uformell ressursallokering kan føre til motstridende prioriteringer, når (minst) et fullt årsverk synes nødvendig.

⁷⁹ «Personvernombud» refererer til personvernombudet på tilsynstidspunktet, også omtalt som «daværende personvernombud» i dokumentet selv om vedkommende ikke lenger innehar denne rollen. Andre steder henviser «personvernombudet» til rollen, uavhengig av om det er det eksterne eller daværende ombudet.

⁸⁰ «Response to Datatilsynet», 13.12.2021, s. 10.

⁸¹ Endelig tilsynsrapport av 30. september 2022, s. 11.

⁸² Endelig tilsynsrapport av 30. september 2022, s. 11.

⁸³ «2021.04.13 – Mail to EVP People». «2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf».

⁸⁴ «2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf», s. 14.

⁸⁵ Endelig tilsynsrapport av 30. september 2022, s. 11.

Telenor ASAs personvernombud nevnte i intervjuet at hun antar at et 50 prosent årsverk vil være hensiktsmessig etter hvert, men at det vil kreve et annet modenhetsnivå med hensyn til personvernet sammenlignet med dagens situasjon.⁸⁶

Videre kom frem i intervjuet at personvernombudet planla å skaffe seg advokatbevilling, noe som ville krevd praktisk prosedyreerfaring fra rettssaker samt advokatkurs. Telenor ASA ville tilrettelegge for prosedyreerfaringen, og den ville antagelig foregå innenfor arbeidstiden.⁸⁷ Telenor ASA har uttalt at de formelle kravene for å tildeles bevilling vil bli oppfylt over tid, avhengig av antall rettssaker, og at det kan ta flere år å opparbeide seg prosedyreerfaring. Videre vil det i hovedsak omfatte mindre saker knyttet til Telenor Norge AS' virksomhet.⁸⁸

Rapporter fra personvernombudet om ressursituasjonen

Personvernombudet tok opp spørsmål om behovet for mer ressurser ved flere anledninger i 2021 og 2022.⁸⁹ For eksempel anbefalte personvernombudet i februar 2021 fortsatt tildeling av:

«100 % FTE on ASA privacy matters (50% DPO, 50% extra) until privacy org./compliance state more mature».⁹⁰

Personvernombudet rapporterte videre på første møtet i GU Forum i september 2021 om følgende:

- «DPO spends 50 % more time than originally intended, while still being overburdened with tasks and being a bottleneck [+P]
- Most time spent on retro-active issue management, instead of pro-active and strategic work [+I/P]
- Internal alignment between CM, BSO and DPO delayed due to capacity and prio [+I/P]
- High-risk processing activities uncovered which should have had a DPIA, but did not (e.g. recording, investigations, tutela) [+I/P]
- Manglende kapasitet til å (tilstrekkelig) håndtere kjente saker [+P]
- Lack of audits and follow-up of contracts makes it a guessing game to assess whether 3rd parties are complying [+I/P]
- Manglende kapasitet og kompetanse til systematisk oppfølging [+I/P]»⁹¹

Disse rapportene fra personvernombudet er i seg selv forhold som tyder på mangel på ressurser.

⁸⁶ Endelig tilsynsrapport av 30. september 2022, s. 11.

⁸⁷ Endelig tilsynsrapport av 30. september 2022, s. 10–11.

⁸⁸ Intervjuer med Telenor ASAs personvernombud [redacted] og leder i Group Legal. Foreløpig tilsynsrapport med merknader fra Telenor ASA i gult, 16. mai 2022, s. 10.

⁸⁹ Endelig tilsynsrapport av 30. september 2022, s. 8–10, 15–16.

⁹⁰ Endelig tilsynsrapport av 30. september 2022, s. 10.

⁹¹ Endelig tilsynsrapport av 30. september 2022, s. 15–16.

I sitt brev av 16. mai 2022 skriver Telenor ASA at behovet for mer ressurser signalisert av personvernombudet har blitt tatt opp av ledelsen, noe som er dokumentert.

Konklusjon

Tilsynet har avdekket at den formelle tildelingen av et 50 prosent årsverk til personvernombudet ikke har vært tilstrekkelig. Videre tyder flere omstendigheter på at det ikke har vært tilstrekkelig at én person har brukt mesteparten av arbeidstiden sin på personvernoppgaver. Vi understreker at personvernombudet ikke er i stand til å utføre alle oppgavene nevnt i personvernforordningen artikkel 39 uten at nødvendige ressurser er stilt til rådighet av arbeidsgiveren i henhold til personvernforordningen artikkel 38 nr. 2. Telenor ASA har i 2021 og 2022 fått på plass flere støttefunksjoner og stilt til rådighet ressurser for å legge til rette for at personvernombudet skal kunne utføre sine oppgaver. Dette var en positiv endring i tilsynsperioden.

Det ovenstående tyder på at det var et etterslep og en generell pulverisering av ansvar og ansvarlighet, med mange spesifikke personvernspørsmål som krevde personvernombudets oppmerksomhet og involvering.⁹² Økningen i ressurser (budsjett til personvern/overholdelse av krav og utnevning av personvernkoordinatorer) kan indirekte støtte personvernombudets rolle, men er ikke tildelt med henblikk på å sikre at personvernombudet kan utføre sine oppgaver.

Datatilsynet legger til grunn at Telenors personvernombud har fått støtte i form av nødvendige ressurser til å opprettholde sin dybdekunnskap.

Ved en helhetsvurdering basert på foreliggende dokumentasjon, intervjuer og opplysninger gitt til forhåndsvarselet, har Datatilsynet under tvil funnet at det er sannsynlighetsovervekt for at Telenor ASA har overtrådt personvernforordningen artikkel 38 nr. 2 ved å ikke stille til rådighet de ressurser personvernombudet trenger for å utføre oppgavene nevnt i artikkel 39, innenfor tilsynsperioden.

8 Personvernombudets tilgang til øverste ledelse, personvernforordningen artikkel 38 nr. 3

8.1 Tilsynskriterier og tilsynsbevis

Personvernforordningen artikkel 38 nr. 3 siste punktum lyder som følger:

«[...] Personvernombudet skal rapportere direkte til det høyeste ledelsesnivået hos den behandlingsansvarlige eller databehandleren.»

Vi viser videre til punkt 3.5.1 og 3.5.2 i den endelige tilsynsrapporten av 30. september 2022.

8.2 Datatilsynets vurdering

I henhold til personvernforordningen artikkel 38 nr. 3 skal den behandlingsansvarlige sikre at personvernombudet rapporterer direkte til «det høyeste ledelsesnivået». Bruken av ordet

⁹² Se punkt 5.2.3.

«høyeste» – superlativformen av «høy» – tyder på at personvernombudet skal rapportere direkte til den øverste ledelsen hos den behandlingsansvarlige eller databehandleren. Hva som regnes som det øverste ledelsesnivået vil avhenge av selskapsform og organisasjonsstruktur i det konkrete tilfellet.

Videre er det ved tolkning av en bestemmelse i EU-retten nødvendig ikke bare å vurdere dens ordlyd, men også sammenhengen den opptrer i og de mål som søkes oppnådd med lovgivningen den inngår i.⁹³ Forarbeidene til personvernforordningen artikkel 38 nr. 3 bør derfor tas i betraktning for å kunne vurdere hva som er den riktige tolkningen av denne bestemmelsen.⁹⁴

Lovgivningsprosessen som førte til at personvernforordningen artikkel 38 nr. 3 ble vedtatt støtter konklusjonen om at personvernombudet skal rapportere direkte til den absolutt øverste ledelsen i organisasjonen. I EU-kommisjonens første utkast til personvernforordningen ble det fastsatt at personvernombudet skulle rapportere til «the management», uten å spesifisere ledelsesnivå.⁹⁵ Europaparlamentet foreslo å erstatte ordet «management» med «executive management».⁹⁶ Europaparlamentet la også til – som et ekstra forbehold – at det skulle utpekes et medlem av toppledelsen som skulle være ansvarlig for at personvernforordningen ble overholdt.⁹⁷

Ordlyden i personvernforordningen artikkel 38 nr. 3 ble ytterligere endret av Det europeiske råd (European Council), og det ble foreslått å spesifisere at rapporteringen skulle rettes til «highest management».⁹⁸ Rådets tilnærming ble til slutt tatt inn i den endelige versjonen av forordningen.

Det legges vekt på spesifisering av ledelsesnivået for å sikre at det høyeste ledelsesnivået i organisasjonen holdes informert om og involveres i hvordan selskapet overholder personvernforordningen og sine egne interne rutiner, og dermed er i stand til å gripe inn for å

⁹³ EU-domstolen sak C-505/19, EU:C:2021:376, avsnitt 77.

⁹⁴ Se blant annet EU-domstolen sak C-621/18, *Wightman m.fl.*, dom 10. desember 2018 (EU:C:2018:999), avsnitt 47, og sak C-548/18, *BGL BNP Paribas*, dom 9. oktober 2019 (ECLI:EU:C:2019:848), avsnitt 25.

⁹⁵ Se EU-kommisjonens første utkast til personvernforordningen (COM/2012/011 final - 2012/0011 (COD)), datert 25. januar 2012, der artikkel 36 nr. 2 (dagens artikkel 38 nr. 3) lyder som følger: «[...] The data protection officer shall directly report to the management of the controller or the processor.» Spørsmålet om potensielle interessekonflikter som kunne oppstå som følge av en rapporteringslinje som var lagt på et for lavt nivå i selskapets hierarki, ble ikke diskutert.

⁹⁶ Se Europaparlamentets utkast til personvernforordningen (EP-PE_TC1-COD (2012)0011), datert 12. mars 2014, der artikkel 36 nr. 2 (dagens artikkel 38 nr. 3) lyder som følger: «[...] The data protection officer shall directly report to the executive management of the controller or the processor.»

⁹⁷ Ibid. Se artikkel 36 nr. 2 (dagens artikkel 38 nr. 3) siste punktum, som lyder som følger: «The controller or processor shall for this purpose designate an executive management member who shall be responsible for the compliance with the provisions of this Regulation.»

⁹⁸ Se Det europeiske råds utkast til personvernforordningen (5419/1/16 REV 1), datert 8. april 2016, der artikkel 38 nr. 3 lyder som følger: «The data protection officer shall directly report to the *highest management level* of the controller or the processor» (vår kursivering). Med denne endringen av spesifikasjonen av ledelsesnivået besluttet Rådet å fjerne Europaparlamentets forslag om å utpeke et medlem av ledelsen som skulle være ansvarlig for overholdelsen av bestemmelsen.

sikre iverksettelse av de tiltak som er nødvendige for å sikre overholdelse.⁹⁹ Henvisningen til øverste ledelsesnivå må også ses i sammenheng med ansvarlighetsprinsippet i personvernforordningen artikkel 5 nr. 2 hvor den behandlingsansvarlige er ansvarlig for å kunne påvise overholdelse av bestemmelsen.

I den forbindelse bør det bemerkes at Artikkel 29-gruppens veiledning om personvernombud fastsetter at:

«[...] artikkel 38, stk. 3, [bestemmer] at databeskyttelsesrådgiveren 'rapporterer direkte til det øverste ledelsesnivå hos den dataansvarlige eller databehandleren'. En sådan direkte indberetning sikrer, at seniorledelsen (f.eks. bestyrelsen) er opmærksom på databeskyttelsesrådgiverens indstilling og henstillinger som en del af databeskyttelsesrådgiverens mission om at informere og rådgive den dataansvarlige eller databehandleren.»¹⁰⁰

Henvisningen til «bestyrelsen» (styret) som et eksempel på toppledelsen må vurderes i lys av organisasjonsstrukturen hos den behandlingsansvarlige eller databehandleren fra sak til sak. Ikke alle behandlingsansvarlige eller databehandlere har et styre. For eksempel vil offentlige myndigheter og organisasjoner som kommuner, fylkeskommuner, universiteter, skoler, statlige organer osv. typisk ikke ha et styre som høyeste ledelsesnivå. Eksemplet i Artikkel 29-gruppens veiledningen må derfor forstås som et konkret eksempel på toppledelsen, som gjelder i de situasjoner der den typen ledelsesstruktur er obligatorisk (typisk for aksjeselskaper og allmennaksjeselskaper), eller rett og slett der den form for ledelsesstruktur er valgt uavhengig av eventuelle obligatoriske krav.

I den foreliggende sak er Telenor ASA organisert som et allmennaksjeselskap underlagt allmennaksjeloven. Selskapet plikter å ha et styre.¹⁰¹ Dette fremgår også av Telenor ASAs organisasjonskart.¹⁰²

Telenor ASA skriver blant annet i sine merknader til forhåndsvarsel av 31. mai 2024:

«Det kan ikke oppstilles noen konkrete krav til hvem det skal rapporteres til, eller hvordan rapporteringen skal foregå.»

«at rapporteringsstrukturen og formatet tilpasses den enkelte virksomhetens "størrelse, organisering og det aktuelle risikobildet", slik at den behandlingsansvarlige har en "fleksibilitet" med hensyn til rapporteringslinjen.»¹⁰³

Datatilsynet understreker at det er virksomhetens ansvar å konkretisere hva som utgjør rapportering til høyeste nivå. Nettopp på grunn av at «høyeste ledelsesnivå» ikke alltid er

⁹⁹ Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2019) s. 344.

¹⁰⁰ WP 243 rev.01 «Retningslinjer for databeskyttelsesrådgivere» vedtatt 13. desember 2016, s. 16.

¹⁰¹ Lov 13. juni 1997 om allmennaksjeselskaper (allmennaksjeloven) §§ 6-1 og 6-12.

¹⁰² <https://www.telenor.com/about/corporate-governance/board-of-directors/>

¹⁰³ Merknader til forhåndsvarsel av 31. mai 2024, s. 36.

entydig blir det desto viktigere med en klar og dokumentert rapporteringslinje til hvem personvernombudet skal rapportere til og hvordan. Dette kommer vi tilbake til i avsnitt 12.2 om artikkel 24.

I denne saken vurderes om Telenor ASA har iverksatt tiltak for å sikre at personvernombudet rapporterer direkte til høyeste ledelsesnivå i Telenor ASA.

Flere tiltak kan være relevante for å sikre overholdelse av personvernforordningen artikkel 38 nr. 3.¹⁰⁴ Etter vårt syn er det viktig å formalisere og forklare personvernombudets rapporteringslinje (i interne dokumenter, for eksempel retningslinjer, rutiner, instruksjer, stillingsbeskrivelser osv.), og sikre at personvernombudet i praksis rapporterer til den øverste ledelsen.

Mellom 2020 og 2022 innførte Telenor ASA flere endringer i sine formelle rutiner, praksis og retningslinjer for personvernombudets rapportering.¹⁰⁵ Under intervjuene som ble foretatt i forbindelse med tilsynet, var Telenor ASA av den oppfatning at det gjennom hele denne perioden var etablert tiltak for å sikre at personvernombudet rapporterte direkte til virksomhetens øverste ledelse. Denne oppfatningen kommer videre frem i Telenor ASA sine merknader til foreløpig tilsynsrapport hvor de skriver:

«For øvrig rapporterer rollen personvernombud til øverste ledelse og lokal policyeier [redacted] gjennom GU forum og ellers slik personvernombudet ser det er nødvendig»¹⁰⁶

Basert på funnene i vårt tilsyn finner vi at Telenor ASAs påstand ikke kan legges til grunn for hele tilsynsperioden i denne saken. Årsakene til dette er beskrevet nedenfor.

For det første må det undersøkes hvordan den øverste ledelsens ansvar for overholdelse av kravene i personvernforordningen artikkel 5 nr. 2 er formalisert.¹⁰⁷ Den funksjonelle stillingsbeskrivelsen til Telenors personvernombud lyder som følger:

«As DPO for Telenor ASA report directly to the highest management level of the Telenor ASA on the status of data protection and urgent matters».¹⁰⁸

Denne ordlyden gjentar bare ordlyden i personvernforordningen artikkel 38 nr. 3 og viser ikke at det foreligger noen direkte forbindelse mellom personvernombudet og det øverste ledelsesnivået i Telenor ASA. Videre er det ikke konkretisert hva som menes med «highest

¹⁰⁴ Se CNPD (datatilsynsmyndigheten i Luxembourg) – vedtak nr. 41 FR/2021 (Délibération N° 41FR/2021 du 27 octobre 2021 – mesure correctrice et amende), avsnitt 68, hvor CNPD i vurderingen av artikkel 38 nr. 3, bemerket at: « Flere tiltak kan vurderes for å oppnå dette resultatet, som for eksempel å knytte personvernombudet til det øverste ledelsesnivået for å sikre maksimal autonomi [for ombudet] eller å opprette en formalisert og regelmessig direktelinje for rapportering, samt en eskaleringsmekanisme for hastesaker til ledelsen som kan omgå eventuelle mellomliggende hierarkiske nivåer.» (Vår oversettelse fra fransk til norsk).

¹⁰⁵ Endelig tilsynsrapport av 30. september 2022, punkt 3.5.2.

¹⁰⁶ «Foreløpig tilsynsrapport – med kommentarer fra Telenor ASA i gult, 16.5.2022», s. 15-16.

¹⁰⁷ Se også i den forbindelse CNPD (Luxembourg) – vedtak nr. 41FR/2021, avsnitt 41 og 42.

¹⁰⁸ «DPO – Functional Job Description – Group Legal – Associate Lawyer & DPO»

management level» i denne sammenheng. En henvisning i stillingsbeskrivelsen til at personvernombudet skal rapportere direkte til den øverste ledelsen er i seg selv ikke tilstrekkelig til å sikre overholdelse av artikkel 38 nr. 3. Vi forventer at organisatoriske tiltak er etablert i dokumenterte interne retningslinjer for personvern med hensyn til hvor, når, hvordan og til hvem personvernombudet skal rapportere. Dette er særlig viktig når Telenor ASA nå hevder at det ikke kan forstås at personvernombudet skal rapportere til selskapets styre.¹⁰⁹ Forståelsen om hva som er «highest management level» må konkretiseres.

Styret er det formelt øverste nivået i Telenor ASA. Uten noen nærmere presisering av rapporteringslinjene er det altså nærliggende å legge til grunn at det er styret som utgjør «highest management level». Telenor ASA påpeker imidlertid i tilsvaret at det etter personvernforordningen ikke er entydig at øverste ledelsesnivå må være styret. I tilsvaret viser Telenor ASA til kommentarutgave til Jarbekk m.fl. som uttaler at personvernombudet ikke skal rapportere til styret fordi styret bare forholder seg til daglig leder, og at «det er ingenting som tyder på at det er meningen at personvernombud skal være likestilt med daglig leder over styret».¹¹⁰ Vi viser her til at EDPB vurderer dette annerledes, og at forarbeidene til forordningen viser at det nettopp er tiltenkt at ombudet skal kunne rapportere til det som reelt er høyeste ledelsesnivå i en virksomhet. Dette er rettskilder som Datatilsynet vurderer har større vekt enn juridisk teori. Hvordan dette står seg mot norsk selskapsrett er ikke omtalt i forarbeidene til personopplysningsloven. Intensjonen er å sikre personvernombudets uavhengighet, og ombudet må dermed kunne rapportere og rådgi uavhengig av formelle linjestrukturer i en virksomhet.

Personvernombudet er tett knyttet til ansvarlighetsprinsippet i artikkel 5 nr. 2.¹¹¹ Ombudet er en rolle basert på “authority and expertise rather than on formal powers over the governance of personal data within organisations”.¹¹² Ombudet har ingen formell rolle overfor styret og har ingen myndighet som går utover virksomhetens, men har en selvstendig rådgivnings- og påpasser rolle med «expert-based autonomy».¹¹³ Det kan være tilfeller hvor det er nødvendig å gjøre styret oppmerksom på personvernrisikoer i virksomheten. Styret skal sørge for forsvarlig organisering av virksomheten, jf. allmennaksjeloven § 6-12 nr. 1, og skal føre tilsyn med den daglige ledelsen og selskapets virksomhet forøvrig, jf. allmennaksjeloven § 6-13 nr. 1. Ansvar etter personvernforordningen artikkel 5 nr. 2 faller dermed formelt på styret, selv om det daglige behandlingsansvaret er lagt til andre i selskapet.

Jarbekk m. fl. skriver videre at det høyeste nivået ikke nødvendigvis betyr *den øverste lederen*, men det høyeste nivået for den daglige ledelsen. Den daglige ledelsen i et allmennaksjeselskap ligger til daglig leder, jf. allmennaksjeloven § 6-14. Det høyeste nivået for den daglige ledelsen er i Telenor ASAs tilfelle CEO eller CEO sammen med

¹⁰⁹ I sine merknader til forhåndsvarsel av 31. mai 2024, s. 37 skriver Telenor ASA: «Det er ikke noe grunnlag for å (i) kreve at personvernombudet skal rapportere til selskapets styre, eller (ii) kreve at den behandlingsansvarlige har formalisert retningslinjer for hvordan og hvem personvernombudet rapporterer til.» (vår kursiv).

¹¹⁰ Eva Jarbekk mfl.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019) s. 337

¹¹¹ Cecilia Alvarez Rigaudias og Alessandro Spina, «Article 38 Position of the data protection officer» i Kuner, Bygrave og Docksey (red) *The EU General Data Protection Regulation (GDPR): A Commentary*, s. 700-708

¹¹² Ibid s. 701.

¹¹³ Ibid s. 703.

vedkommendes ledergruppe (Group Leadership Team). Hvis vi legger denne forståelsen av det høyeste nivået til grunn, vil det være naturlig at personvernombudet rapporterer til CEO eller CEO sammen med Group Leadership Team. Det kan argumenteres for at en slik tolkning ivaretar formålet til bestemmelsen idet den øverste daglige ledelsen vil være nærmest til å agere på bakgrunn av personvernombudets rapport, nettopp fordi vedkommende utøver operativ ledelse over selskapet på daglig basis.

Tilsvaret viser videre til at Jarbekk m.fl. presiserer at det foreligger en viss fleksibilitet i de nøyaktige rapporteringslinjene, men er ikke konkret på om dette betyr at rapporteringen kan legges til nivåer under den høyeste ledelsen.¹¹⁴ En slik forståelse vil gå lenger enn det som er mulig å lese ut fra lovens ordlyd og intensjon som med høyeste ledelsesnivå klart legger rapporteringen til det høyeste og ikke ethvert ledelsesnivå. Vi mener en slik utvidende tolkning ikke kan legges til grunn.

Som EU domstolen har uttalt: «som det følger af fast retspraksis, skal der ved fortolkningen af en EU-retlig bestemmelse tages hensyn til ikke alene dens ordlyd i overensstemmelse med dens sædvanlige betydning i almindelig sprogbrug, men også til den sammenhæng, hvori den indgår, og til de mål, der forfølges med den ordning, som den udgør en del af.»¹¹⁵ Øverste ledelsesnivå må derfor tolkes i lys av lovens intensjon som er å «sikre et højt niveau for beskyttelse af fysiske personer inden for Unionen, og med henblik herpå sikre, at reglerne for beskyttelse af disse personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af personoplysninger anvendes konsekvent og ensartet overalt i Unionen.»¹¹⁶

Vi viser også til at referansen i tilsvaret til Voigt og Bussche ikke sier at det *ikke* skal rapporteres til høyeste nivå, men at det ikke er nødvendig at «each and every routine data protection matter» blir rapport til øverste ledelsesnivå. Samtidig understreker de at personvernombudet «must be able to report directly to the highest management level when the need arises and must not be prevented from doing so by the organisation». Slik vi ser det kan personvernombudet i det daglige kommuniserer med ulike nivåer i organisasjonen, men selve rapporteringen skal kunne skje direkte til det høyeste ledelsesnivået. Her er det viktig å skille mellom involvering av personvernombudet etter artikkel 38 nr. 1 – som bør skje på flere ulike nivåer, og der personvernombudet står nærmest til å vurdere hva som er hensiktsmessig – og den formelle rapporteringen etter artikkel 38 nr. 3.

Etter Datatilsynets syn vil rapportering til styret oppfylle kravet etter artikkel 38 nr. 3 siste punktum. Datatilsynet er også åpen for at rapportering til CEO eller rapportering til CEO sammen med vedkommendes ledergruppe kan oppfylle kravet. En slik rapportering forutsetter imidlertid at personvernombudet kan eskalere saker videre til styret fordi ansvaret etter personvernforordningen artikkel 5 nr. 2 som nevnt faller på styret.

Det er uansett viktig å gjennomføre en konkret vurdering av personvernombudets rapporteringslinje og dokumentere denne, noe som vi anser mangelfullt i denne saken. Vi viser til punkt 12 nedenfor.

¹¹⁴ Eva Jarbekk mfl.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019) s. 337

¹¹⁵ EU-domstolen sak C-453/21, *X-FAB Dresden*, avsnitt 19 og EU domstolen sak, C-534/20 *Leistriz*, avsnitt 18.

¹¹⁶ EU-domstolen sak C-453/21, *X-FAB Dresden*, avsnitt 25 og EU domstolen sak, C-534/20 *Leistriz*, avsnitt 26.

Det kom frem i intervjuene med det eksterne og det daværende personvernombudet, samt ledelsen,¹¹⁷ at personvernombudet rapporterte til ██████████, Executive Vice President and Chief People and Sustainability Officer i første delen av tilsynsperioden. Telenor ASA innså at det var behov for bredere rapportering enn bare til henne, og det var lagt opp til at personvernombudet kunne rapportere til CCM (Compliance Committee Meetings).¹¹⁸ Videre kom det frem i intervjurunden at det eksterne personvernombudet gjorde Telenor ASA oppmerksom på at CCM, som var på konsernnivå, «nok ikke var den optimale kontakten med ledelsen» i Telenor ASA.

For det andre fastsetter låneavtalen mellom Telenor ASA og ██████████ for ansettelse av det eksterne personvernombudet fra januar 2021 til oktober 2021 at personvernombudet skal rapportere til «██████████, VP Privacy and Information Management Telenor Group».¹¹⁹ Dette er bare en henvisning til den ansattes linjeledelsesrapportering, ikke personvernombudets rapporteringslinje for personvernspørsmål.¹²⁰ ██████████ hadde heller ikke ansvar for overholdelse av krav i Telenor ASA, men på konsernnivå.

For det tredje har Telenor ASA en konsernhåndbok i personvern («Group Manual Privacy») og en konsernpolicy for personvern («Group Policy Privacy») som skal sikre overholdelse av krav i konsernet, herunder i Telenor ASA. I forbindelse med tilsynet har vi mottatt både de oppdaterte retningslinjene datert 1. januar 2022 (som ble gyldig etter at Datatilsynet varslet sitt tilsyn 26. november 2021) og de gamle mandatene og retningslinjene (gyldig i perioden fra 1. juni til 31. desember 2021).¹²¹ I den forbindelse beskriver håndboken og mandatet noen skriftlige rutiner for GPOs («Group Privacy Officer») rapportering om personvern til ledelsen, for eksempel til «Chief Compliance Officer» og til konsernsjefen (CEO) gjennom «Group Compliance Committee» (GCC).¹²²

Mellom 1. mars 2020 og 30. november 2021 jobbet en gruppe kalt Group Unit for Privacy & IM i Compliance-avdelingen med personvern i Telenor-konsernet.¹²³ I det interne dokumentet om gruppens mandat står følgende:

«Group Privacy & IM has a preventive, advisory and supervisory role, acting independently from operational management, with particular emphasis on three main areas of responsibility:

- a) Act as Group Policy Manager for Privacy & IM, in accordance with Telenor's Compliance Management System to ensure that the applicable Group Manuals

¹¹⁷ Intervjuer av 28. januar 2022 med ██████████

¹¹⁸ Se vedtakets punkt 6.2.

¹¹⁹ «DPO – ██████████ Loan staff agreement ██████████ DPO jan 21 - oct 21»

¹²⁰ Endelig tilsynsrapport av 30. september 2022, s. 17.

¹²¹ For ytterligere opplysninger om mandatene, håndbøkene og retningslinjene, se den endelige tilsynsrapport av 30. september 2022, punkt 7.2.2 s. 18–19.

¹²² «Group Manual Privacy, valid from 1 June 2020», s. 3–4, «2020 Mandate and Functional Description Group Privacy and IM (share), valid from: 01.03.2020», s. 3. Vi forstår det slik at Group Compliance Committee er det samme som «CCM» eller Compliance Committee Meeting som Telenor ASA henviste til.

¹²³ «2020 Mandate and Functional Description Group Privacy and IM (share), valid from: 01.03.2020». Gyldig til 30. november 2021, se «Response to Datatilsynet additional documentation», 10.01.2022, s. 2–3.

are kept up to date and are being effectively adopted across the Group. Group Privacy & IM shall perform core CMS activities following a Plan-Do-Check-Act model, and the implementation of the Group Manuals are subject to monitoring and management reporting, as described in chapter 4.

- b) *Act as both the Group Privacy Officer and DPO for Telenor ASA*, including the right and duty to report independently on relevant privacy risks and non-conformities to the Group President and CEO of Telenor. (Vår kursivering).
- c) Advise and support management at the Group-level, and other key stakeholders such as Data Protection Officers (DPOs) in the BUs. Advisory and support tasks include:
 - Providing expertise and knowledge on specific privacy and IM topics
 - Providing expertise and input on privacy and IM advocacy activities
 - Providing expertise and input on privacy strategy and position development
 - Supporting the implementation of privacy and IM requirements in relevant Group-wide processes.»¹²⁴

Det kommer fram at GPO kan rapportere til styret via «Sustainability and Compliance Committee.»¹²⁵ I sitt svar til Datatilsynet understreker Telenor ASA imidlertid at rollene til personvernombudet og GPO – til tross for den ordlyden i mandatet – var helt atskilt og ivaretatt av to ulike personer.¹²⁶ Videre opplyser Telenor ASA at henvisningen til at «Group Privacy & IM» fungerer som både GPO og personvernombudet for Telenor ASA bare var ment som en henvisning til sistnevntes organisatoriske tilknytning til enheten, og at personvernombudets ansvar, oppgaver og rapporteringslinjer ikke var beskrevet i dokumentet.¹²⁷ Telenor ASA har dokumentert at ovennevnte stillingene var besatt av forskjellige individer.¹²⁸ Datatilsynet bemerker at denne konsernhåndboken og mandatet da ikke inneholdt noen spesifikke føringer for personvernombudet i Telenor ASA, noe vi anser som mangelfullt.

For det fjerde er det vår vurdering at Telenor ASAs mangel på en formalisert rapporteringslinje har gitt personvernombudet praktiske problemer med å utføre sine oppgaver i henhold til personvernforordningen. Det eksterne personvernombudet uttalte under tilsynet vårt at han opplevde manglende tilgang til den øverste ledelsen.¹²⁹ Videre understreket det eksterne personvernombudet at han opplevde mangel på organisasjonsmessig effektivitet, og at han var frustrert på grunn av de mange hierarkiske nivåene personvernombudet måtte omgå og involvere for å nå toppledelsen.¹³⁰

I den forbindelse bemerker vi at personvernombudets praktiske vanskeligheter med å omgå hierarkiske mellomledd og rapportere direkte til den øverste ledelsen i seg selv har blitt ansett

¹²⁴ «2020 Mandate and Functional Description Group Privacy and IM (share), valid from: 01.03.2020», s. 2.

¹²⁵ «2020 Mandate and Functional Description Group Privacy and IM (share), valid from: 01.03.2020», s. 3.

¹²⁶ Endelig tilsynsrapport av 30. september 2022, s. 17–18 og 12–13

¹²⁷ Endelig tilsynsrapport av 30. september 2022, s. 13.

¹²⁸ «Foreløpig tilsynsrapport – med kommentarer fra Telenor ASA i gult, 16.5.2022», s. 11.

¹²⁹ Endelig tilsynsrapport av 30. september 2022, s. 18.

¹³⁰ Endelig tilsynsrapport av 30. september 2022, s. 18.

som et brudd på personvernforordningen artikkel 38 nr. 3 av andre tilsynsmyndigheter.¹³¹ Telenor ASA hevder i tilsvaret at «vedtak fattet av en utenlandsk tilsynsmyndighet er av liten rettslig relevans, særlig når Datatilsynet ikke har påvist at vedtaket utgjør noen fast praksis.»¹³² Vi er ikke enig i denne påstanden. Personvernforordningen gjelder i hele EØS, og ifølge fortalepunkt 13 har den som mål å sikre likt vern av individer, sikre ensartet tilsyn med behandling av personopplysninger og samme sanksjoner i alle medlemsland m.m. Vi mener det er relevant å se hen til praksis i andre EØS-land siden det forutsettes at fortolkningen av personvernforordningen er harmonisert.

Det eksterne personvernombudets rapport om personvernstatus og forslag til Telenor ASA i GU Forum 2021 oppgir:

«a) DPO reporting, access & independence -The DPO is unable to perform the role effectively and independently due lack of proper implementation of the role in the organization, including clarified reporting lines, access to highest level of management and interference in reporting.»¹³³

I den samme rapporten ble det videre gjort følgende observasjoner:

- «DPO reporting and sounding board not implemented
- Independent reporting and mgmt. access (has been) difficult»¹³⁴

Som et oppfølgingspunkt fra personvernombudet ble det fremhevet at Telenor ASA må:

«Establish DPO reporting line to ASA mgmt.»¹³⁵

Disse uttalelsene og funnene fra det eksterne personvernombudet illustrerer kjerneproblemet når den behandlingsansvarlige ikke sikrer formalisering av personvernombudets rapporteringslinje til den øverste ledelsen. Det eksterne personvernombudet hadde på det tidspunktet ikke mulighet til å henvise til håndbøkene eller retningslinjene for å kreve sin rett til direkte kontakt med den øverste ledelsen. Det ble heller overlatt til personvernombudets eget initiativ å involvere og omgå hierarkiske nivåer for å nå den øverste ledelsen. Selv om uformell kontakt med den øverste ledelsen teknisk sett kan ha vært mulig, kan det dermed ikke anses som overholdelse i denne saken.

For ordens skyld merker vi oss at Telenor ASAs ledelse i intervjuet erkjente at det ikke var tilstrekkelig å bare rapportere til «Privacy Policy Owner». De så behovet for endringer i personvernombudets rapporteringslinje. Ledelsen besluttet dermed at personvernombudet

¹³¹ Se f.eks. CNPD (Luxembourg) – vedtak nr. 20FR/2021, avsnitt 37 til 43.

¹³² Merknader til forhåndsvarsel av 31. mai. 2024, s. 38.

¹³³ «2021.09.09 – TNASA Privacy status and proposals for GU Forum», s. 13.

¹³⁴ «2021.09.09 – TNASA Privacy status and proposals for GU Forum», s. 13.

¹³⁵ «2021.06.10 – TNASA Privacy status and proposals_FINAL», s. 5.

kunne rapportere kvartalsvis til «CCM»,¹³⁶ og fra sommeren 2021 ble denne rapporteringslinjen erstattet av GU Forum med første møte i september 2021.¹³⁷

I den forbindelse merker vi oss at «Privacy Policy Owner» – dvs. [REDACTED] og senere [REDACTED] – på det tidspunktet var en del av «Group Executive Management» (et rådgivende organ for konsernsjefen) og hadde henholdsvis titlene «Executive Vice President and Chief People and Sustainability Officer» og «Executive Vice President Strategy & External Relations». Dette kan ikke anses som øverste ledelse i henhold til personvernforordningen artikkel 38 nr. 3.

Når det gjelder CCM, påpekte det eksterne personvernombudet at dette forumet ikke var egnet som hovedrapporteringskanal fra personvernombudet til Telenor ASAs øverste ledelse.¹³⁸ Disse møtene var innrettet for å ta opp spørsmål om overholdelse av krav på konsernnivå, og at saker om personvernrisikoer i Telenor ASA ble lettvektere sammenlignet med andre temaer og punkter på dagsordenen angående problemstillinger på konsernnivå.¹³⁹ Dette gjenspeiles også i at personvernombudet ikke hadde noe formelt eller fast punkt på agendaen til å ta opp personvernspørsmål vedrørende Telenor ASA.¹⁴⁰ Hvis personvernombudet rapporterte til CCM, var dette bare ad hoc, og det var opp til personvernombudet å be om å få delta på møtene.¹⁴¹ I den forbindelse merker vi oss at Telenor ASA kun har levert referat fra *ett* CCM-møte som inneholder informasjon eller rapportering fra personvernombudet. Det er også verdt å nevne at personvernombudet ikke fikk mulighet til å delta personlig, og presentasjonen som var utarbeidet for CCM ble distribuert i forkant av møtet til orientering og ikke for diskusjon på møtet.¹⁴²

Det første møtet i GU Forum som personvernombudet deltok i, ble avholdt i september 2021, og dagsordenen omfattet personvernspørsmål knyttet spesifikt til Telenor ASA,¹⁴³ noe som var en positiv endring fra CCM.

GU Forum ble opprettet som hovedarena for rapportering og dialog om personvernspørsmål med ledelsen i Telenor ASA.¹⁴⁴ GU Forum ble ledet av avdelingslederen («Executive Vice President») for «People & Sustainability» og besto av lederne for de andre avdelingene i Telenor ASA, såkalte «Group Units».¹⁴⁵ I intervjuet ble GU Forum beskrevet som en arena der «Executive Vice Presidents» kan bli enige om beslutninger som skal tas i linjeorganisasjonen, og forumet kan ikke anses som et eget beslutningsorgan.¹⁴⁶ GU Forum

¹³⁶ Angående «Compliance Committee Meeting», se punkt 6.2.

¹³⁷ Se endelig tilsynsrapport av 30. september 2022, side 19, som fastslår at overgangen fra CCM til GU Forum var en direkte konsekvens av det eksterne personvernombudets fortsatte innsats for å informere og rapportere til ledelsen og «Privacy Policy Owner» om mangelen på klare, formelle rapporteringslinjer til høyeste ledelsesnivå.

¹³⁸ Endelig tilsynsrapport av 30. september 2022, s. 18.

¹³⁹ Ibid.

¹⁴⁰ Endelig tilsynsrapport av 30. september 2022, s. 18–19.

¹⁴¹ Ibid.

¹⁴² Endelig tilsynsrapport av 30. september 2022, s. 18.

¹⁴³ «2021.12.03 - TNASA GU Forum re. privacy - scope and mandate_final»

¹⁴⁴ Ibid.

¹⁴⁵ «Overview of DPO role and reporting lines», s. 2.

¹⁴⁶ Endelig tilsynsrapport av 30. september 2022, s. 20.

består dermed av ledere i Telenor ASA, hvorav Executive Vice President for Strategy & External Relations også sitter i ledelsen i Telenor ASA og i konsernet.¹⁴⁷

Det fremgår av dokumentasjonen vi har mottatt at GU Forum ikke har beslutningsmyndighet. Dette i seg selv tilsier at GU Forum ikke kan anses som det øverste ledelsesnivået i personvernforordningens forstand. For øvrig bemerker vi at å rapportere til enkeltpersoner som sitter i ledelsen ikke er det samme som å rapportere til ledelsen som sådant.

Datatilsynet merker seg at Telenor ASA nevner i et par PowerPoint-presentasjoner om personvernorganiseringen at personvernombudet kan eskalere og rapportere saker direkte til «CEO 1. escalation» og «BoD 2. escalation» (styret). Disse er datert 6. desember 2021 eller etter vårt varsel om tilsyn ble sendt.¹⁴⁸ Dette er en positiv endring, men vi bemerker at Telenor ASA ikke har lagt frem noe informasjon om hvordan disse rapporteringslinjene fungerer i praksis. For å oppfylle kravet om interne retningslinjer i art. 24 nr. 2 mener vi at informasjonen som fremkommer av lysbildene også bør nedtegnes i relevante retningslinjer da lysbilder alene ikke nødvendigvis oppfyller dette kravet. Retningslinjer må være tilgjengelige og kjente i organisasjonen. Vi bemerker at Telenor ASA med bistand fra personvernombudet, gjorde en innsats for å rette og forbedre rapporteringslinjer for personvernombudet til øverste ledelse. Videre viser lysbildene at måneden før vi gjennomførte intervjuer hadde Telenor ASA innsett at det burde være en rapporteringslinje for å melde saker til både styret og CEO.¹⁴⁹ Telenor ASAs forsøk på utbedring endrer dog ikke at i nesten et år manglet personvernombudet direkte rapporteringslinje til øverste ledelse, slik det har kommet frem ovenfor.

Samlet sett har de ovennevnte omstendighetene ført til at Datatilsynet vurderer at Telenor ASA, i største del av tilsynsperioden, ikke hadde direkte rapporteringslinje til det øverste ledelsesnivået, og har overtrådt personvernforordningen artikkel 38 nr. 3. Se også punkt 3.5.3 i endelig tilsynsrapport av 30. september 2022.

9 De registrertes tilgang til personvernombudet, artikkel 38 nr. 4

9.1 Tilsynskriterier og tilsynsbevis

Personvernforordningen artikkel 38 nr. 4 lyder som følger:

«De registrerte kan kontakte personvernombudet angående alle spørsmål om behandling av deres personopplysninger og om utøvelsen av de rettighetene de har i henhold til denne forordning.»

Vi viser videre til punkt 3.6.1 og 3.6.2, i tillegg til punkt 3.1.2, i den endelige tilsynsrapporten av 30. september 2022.

¹⁴⁷ Merknader til forhåndsvarsel av 31. mai 2024, s. 39.

¹⁴⁸ «TNASA Privacy organisation overview», per 2021.12.06 og «2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf»

¹⁴⁹ Se i denne sammenhengen f.eks. CNPD (Luxembourg) – vedtak nr. 20FR/2021, avsnitt 39, som uttaler at personvernombudet bør kunne omgå de mellomliggende hierarkiske nivåene der det anses som nødvendig.

9.2 Datatilsynets vurdering

Formålet med personvernforordningen artikkel 38 nr. 4 er å fastslå de registrertes rettigheter i forbindelse med kontakt til personvernombudet. Den er nært forbundet med personvernforordningen artikkel 37 nr. 7. Vi anser det som en forutsetning for at de registrerte skal kunne kontakte personvernombudet angående alle spørsmål som gjelder behandling av personopplysninger og om utøvelsen av deres rettigheter, at kontaktopplysningene til personvernombudet er lett tilgjengelige.

Vi viser til punkt 5.2.4 i dette vedtaket, der vi påpeker et brudd. Bortsett fra dette fant ikke Datatilsynet noe annet under tilsynet som tydet på at denne rettigheten for de registrerte ikke var sikret.

10 Personvernombudets uavhengighet og fravær av interessekonflikter, artikkel 38 nr. 3 og 6

10.1 Tilsynskriterier og tilsynsbevis

Personvernforordningen artikkel 38 nr. 3 første og andre punktum lyder som følger:

«Den behandlingsansvarlige og databehandleren skal sikre at personvernombudet ikke mottar instruksjoner om utførelsen av nevnte oppgaver. Vedkommende skal ikke avsettes eller straffes av den behandlingsansvarlige eller databehandleren for å utføre sine oppgaver.»

Vi viser videre til punkt 3.4.1 og 3.4.2 i den endelige tilsynsrapporten av 30. september 2022, særlig der det står at det eksterne personvernombudet informerte oss om at han aldri mottok noen direkte instruksjoner fra ledelsen om utøvelsen av sine oppgaver. Under tilsynet fant Datatilsynet ingen dokumentasjon på at noe personvernombud i Telenor ASA hadde blitt avsatt eller straffet av Telenor ASA for å utføre sine oppgaver.

Videre lyder personvernforordningen artikkel 38 nr. 6 som følger:

«Personvernombudet kan utføre andre oppgaver og ha andre plikter. Den behandlingsansvarlige eller databehandleren skal sikre at nevnte oppgaver eller plikter ikke fører til en interessekonflikt.»

Vi viser videre til punkt 3.7.1 og 3.7.2 i den endelige tilsynsrapporten av 30. september 2022.

10.2 Datatilsynets vurdering

Vi anser personvernforordningen artikkel 38 nr. 3 og 6 for å være nært beslektet og vurderer derfor begge bestemmelsene i dette avsnittet.

Personvernforordningen artikkel 38 nr. 3 fastsetter at den behandlingsansvarlige skal sikre at personvernombudet ikke mottar instruksjoner om utførelsen av sine oppgaver. Denne bestemmelsen er viktig for å sikre personvernombudets uavhengighet.¹⁵⁰ Den viser ikke bare til direkte instruksjoner fra en overordnet, men også at et personvernombud ikke må settes i en posisjon der vedkommende er tilbøyelig til å godta visse kompromisser i saker som involverer ansatte i høyere stillinger hos den behandlingsansvarlige.¹⁵¹

Artikkel 38 nr. 6 fastsetter at «personvernombudet kan utføre andre oppgaver og ha andre plikter», forutsatt at «slike oppgaver eller plikter ikke fører til en interessekonflikt».¹⁵² Det er derfor sentralt at personvernombudets uavhengighet garanteres, særlig når personvernombudet får andre oppgaver i organisasjonen. Grunnen til dette er, som påpekt av «Network of Data Protection Officers of the EU Institutions and Bodies», at «a part-time DPO faces a permanent conflict between allocating time and efforts to their DPO tasks versus other tasks [and is] in danger of encountering conflicts of interest».¹⁵³ Det er derfor særdeles viktig å gjøre grundige vurderinger om mulig interessekonflikt når det opprettes en deltidsstilling som personvernombud.

For å unngå interessekonflikter bør behandlingsansvarlige sørge for å:

- «identifisere de stillinger, som er uforenelige med databeskyttelsesrådgiverens funksjoner
- utarbejde interne regler herom for at unngå interessekonflikter
- inkludere en mere generell forklaring om interessekonflikter
- erklære, at deres databeskyttelsesrådgiver ikke befinner seg i en interessekonflikt med hensyn til funksjonen som databeskyttelsesrådgiver med henblik på at øge bevidstheden om dette krav
- inkludere sikkerhedsforanstaltninger i organisationens interne regler og sikre, at opslaget af stillingen som databeskyttelsesrådgiver eller tjenesteydelseskontrakten er tilstrækkeligt præcist og detaljeret til at unngå en interessekonflikt. I denne sammenhæng bør det også tages i betragtning, at interessekonflikter kan antage forskellige former afhængigt af, om databeskyttelsesrådgiveren er rekrutteret internt eller eksternt.»¹⁵⁴

¹⁵⁰ Se fortalepunkt 97, som fastslår at «[...] personvernombud, enten de er ansatt hos den behandlingsansvarlige eller ikke, bør kunne utføre sine funksjoner og oppgaver på en uavhengig måte.»

¹⁵¹ Se ved analogi EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies (30. september 2018), s. 9.

¹⁵² WP 243 rev.01 «Retningslinjer for databeskyttelsesrådgivere» vedtatt 13. desember 2016, s. 17 (der følgende fastslås: «Undgåelse af interessekonflikter er tæt knyttet til kravet om uafhængighed i udførelsen af opgaverne. Selvom det er tilladt databeskyttelsesrådgivere at have andre funktioner, må de kun tildeles andre opgaver og pligter, forudsat at disse ikke giver anledning til interessekonflikter»).

¹⁵³ Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (14 October 2010), s. 6. Se også EDPS Position paper on the role of Data Protection Officers of the EU institutions and bodies (30. september 2018), s. 9.

¹⁵⁴ WP 243 rev.01 «Retningslinjer for databeskyttelsesrådgivere» sist revidert og vedtatt 5. april 2017, godkjent av EDPB i Endorsement 1/2018 av 25. mai 2018, s. 17.

I den foreliggende sak har Telenor ASAs personvernombud også andre oppgaver. Som Telenor ASA bemerker:

«The DPO is organizationally situated within the Group Legal department (a Group Unit) and has its personnel line reporting here. The DPO is appointed as a 50 % FTE position, while this person's remaining 50 % FTE is allocated to being an associate lawyer for Group Legal».¹⁵⁵

Det bør derfor vurderes om en slik ordning er forenlig med personvernforordningen artikkel 38 nr. 3 og 6, og om Telenor ASA har truffet tiltak for å unngå mulige interessekonflikter.

Telenors konsernhåndbok i personvern (Group Manual Privacy) fra 2020 fastslår følgende:

«The BU shall ensure that the DPO is in a position to perform her or his duties and tasks in an independent manner and shall not receive any instructions regarding the exercise of these tasks. He or she shall not be dismissed or penalised by Telenor for performing his/her tasks. To avoid any conflicts of interests, the DPO cannot be organised in the line-organisation, but shall be organised in the Corporate Affairs Unit of the BU and report directly to the Corporate Affairs Officer of the BU»¹⁵⁶.

Group Manual Privacy fra 2020 gjenspeiler i hovedsak ordlyden i personvernforordningen artikkel 38 nr. 3 og 6 samt fortalepunkt 97.

Group Policy Privacy og Group Manual Privacy fra 2022 inneholder mindre detaljerte beskrivelser i så henseende, ettersom de nevner at personvernombudet bør være «uavhengig», men ikke spesifiserer at personvernombudet bare kan utføre andre oppgaver og plikter dersom det ikke fører til en interessekonflikt.¹⁵⁷

Uansett er en henvisning til personvernombudets uavhengighet i interne retningslinjer i seg selv ikke tilstrekkelig til å sikre overholdelse av personvernforordningen artikkel 38 nr. 3 og nr. 6. For å bekrefte om den behandlingsansvarlige har truffet tilstrekkelige tiltak for å sikre at personvernombudet kan utføre sine oppgaver på en uavhengig måte, og at tilleggsoppgaver og -plikter ikke fører til en interessekonflikt, må også andre faktorer vurderes. Særlig bør det vurderes om det er forhold som kan svekke personvernombudets stilling, og om de andre oppgavene personvernombudet blir bedt om å utføre innebærer å fremme interesser som kan komme i konflikt med personvern hensyn.

Selv om det ikke er uvanlig for deltidsansatte personvernombud å være en del av organisasjonens juridiske team, omfatter oppgaver som normalt tilligger et slikt team også

¹⁵⁵ «Response to Datatilsynet», 13. desember 2021, s. 10.

¹⁵⁶ «Group Manual Privacy, Valid from: 01.06.2020», punkt 1.2.2.

¹⁵⁷ «Group Manual Privacy, Valid from: 2022-01-01», punkt 1.1., «Group Policy Privacy, Valid from: 2022-01-01», punkt 2.1.

oppgaver som kan føre til interessekonflikter for personvernombudet.¹⁵⁸ Når personvernombudet er en del av det juridiske teamet, er det derfor avgjørende å sikre at personvernombudet bare gis andre oppgaver eller plikter som er forenlige med rollen som personvernombud. Det må være åpenbart – både for personvernombudet og resten av organisasjonen – hvilke oppgaver vedkommende utfører i egenskap av sin rolle som henholdsvis personvernombud og medlem av det juridiske teamet. Artikkel 29-gruppen/Personvernrådet har i den forbindelse uttalt at en viktig faktor for å unngå interessekonflikter er å sikre at «stillingen som databeskyttelsesrådgiver eller tjenesteydelseskontrakten er tilstrøkkelig præsist og detaljert».¹⁵⁹ Datatilsynet for EU-organene (European Data Protection Supervisor, «EDPS») har uttalt at:

«If the DPO is also a member of the legal team, organisational measures should be put in place to allow the DPO and their staff to clearly distinguish their activities, e.g. by having a separate functional mailbox for DPO matters (so that the rest of the organisation can see whether the advice comes from the DPO function or legal advisory function).»¹⁶⁰

Vi mener at de organisatoriske tiltakene Telenor ASA har iverksatt ikke sikrer et tydelig skille mellom oppgavene som skal utføres som henholdsvis personvernombud og advokatfullmektig.

Telenor ASAs funksjonelle stillingsbeskrivelse for den som skal ansettes som personvernombud og advokatfullmektig («DPO & Associate Lawyer») beskriver medarbeiderens ansvar («responsibility») på følgende måte:

«Implement and/or develop as necessary policies, manuals, best practices, provide legal advice, and liase with external legal counsel. This shall be done in line with the risks and tasks identified by the Heads of Legal for Telenor Digital/Nordic Content/Technologies & Services/Telenor Norway and the prioritizations set by Head of Group Legal and Team Leader for Contracts & Content Team.

- Inform and provide legal advice in alignment with other attorneys in Group Legal to Telenor ASA and the employees on their obligations pursuant to Data Protection Laws, regulations and other requirements.
- Provide advice as regards the data protection impact assessment;
- Cooperate with the supervisory authority;
- Act as the contact point for the data protection supervisory authority on issues relating to processing, and to consult, where appropriate, with regard to any other matter.

¹⁵⁸ For eksempel kan det oppstå en interessekonflikt dersom et personvernombud blir bedt om å representere den behandlingsansvarlige i retten i saker som gjelder vern av personopplysninger, se WP 243 rev.01 Retningslinjer for databeskyttelsesrådgivere vedtatt 13. desember 2016, godkjent av EDPB i Endorsement 1/2018 av 25. mai 2018, s.17.

¹⁵⁹ Ibid.

¹⁶⁰ EDPS, Position paper on the role of Data Protection Officers of the EU institutions and bodies (30. September 2018), s. 11.

- On behalf of Telenor ASA seek prior consultation, where required, for high risk processing in absence of sufficient measures to mitigate such risk
- As DPO for Telenor ASA report directly to the highest management level of the Telenor ASA on the status of data protection and urgent matters». ¹⁶¹

Videre er medarbeiderens oppgaver («tasks») beskrevet slik i den funksjonelle stillingsbeskrivelsen:

«Implement and/or develop as necessary policies, manuals, best practices, provide legal advice (including contribute in relation to Authority Requests) and provide support during negotiations of contracts and liase with external legal counsel. Cooperate closely with other experts in Group Legal and other Group functions as required to support high risk or critical processes. Share information and best practice with colleagues in Group Legal.

Act as DPO in accordance with the GDPR which entail the following activities as examples:

- Develop and maintain Privacy Management Tools and Data Transfer Mechanisms
- Contribute to Training and Awareness Program
- Contribute to embed Data Privacy Into Operations
- Inform and Advise on Data Protection Impact Assessments
- Inform and Advise on Integrating Privacy by Design into Data Processing Operations
- Contribute to management of Third-Party Privacy Risks
- Contribute to Privacy Notices
- Inform and Advise on Requests and Complaints from Data Subjects
- Monitor for New Operational Practices
- Develop and Evolve the Relevant Guidelines and Templates to Support Telenor ASA in Matters Regarding Protection of Personal Data
- Liaise with Group Compliance on related compliance activities». ¹⁶²

Selv om det er en tom linje i Excel-arket som skiller de to avsnittene, mener vi at dette ikke er tilstrekkelig til å tydelig skille mellom oppgavene som skal utføres som henholdsvis personvernombud og advokatfullmektig. Telenor ASA hevdet imidlertid etter vårt tilsyn at bare de oppgavene som er uttrykkelig oppført i den funksjonelle stillingsbeskrivelsen som eksempler på personvernombudets aktiviteter, skal utføres som personvernombud, mens de andre oppgavene skal utføres som advokatfullmektig. Denne uttalelsen som ble gjort i ettertid for å klargjøre den relevante oppgavefordelingen, bøter ikke på tvetydigheten i den funksjonelle stillingsbeskrivelsen. For eksempel hevder Telenor ASA at det er utelukkende i egenskap av rollen som advokatfullmektig at den ansatte skal:

«Implement and/or develop as necessary policies, manuals, best practices [...] in line with the risks and tasks identified by the Heads of Legal for Telenor Digital/Nordic

¹⁶¹ DPO - Functional Job Description - Group Legal - Associate Lawyer & DPO – Excel.

¹⁶² DPO - Functional Job Description - Group Legal - Associate Lawyer & DPO – Excel.

Content/Technologies & Services/Telenor Norway and the prioritizations set by Head of Group Legal and Team Leader for Contracts & Content Team».¹⁶³

Dette selv om et av eksemplene på personvernombudets oppgaver i den funksjonelle stillingsbeskrivelsen er «Develop and Evolve the Relevant Guidelines and Templates to Support Telenor ASA in Matters Regarding Protection of Personal Data». Tilsvarende hevder Telenor ASA at det er i egenskap av rollen som advokatfullmektig at den ansatte skal «Inform and provide legal advice in alignment with other attorneys in Group Legal to Telenor ASA and the employees on their obligations pursuant to Data Protection Laws, regulations and other requirements»,¹⁶⁴ selv om denne ordlyden i hovedsak gjenspeiler ordlyden i personvernforordningen artikkel 39 nr. 1 bokstav a om personvernombudets oppgaver.¹⁶⁵ Det siste elementet gir særlig grunn til bekymring, da det antyder at personvernombudets råd om personvernsspørsmål skal være «in alignment with other attorneys in Group Legal», noe som strider mot kravet om at personvernombudet skal opptre uavhengig.

Vi presiserer at det å jobbe som advokat per se ikke utelukker å kunne gjennomføre personvernombudsoppgaver, for eksempel hvis den juridiske rådgivningen handler om andre rettsområder enn personvern i selskapet.¹⁶⁶ Det blir en enkeltvurdering i hver sak¹⁶⁷ og det er ikke til å unngå at rammene må være klare og tydelige.

Telenor ASA fremhever EU-domstolens avgjørelse i sak C-453/21 *X-FAB Dresden*, hvor det blant annet uttales:

«der kan foreligge en «interessekonflikt» som omhandlet i denne bestemmelse, når en databeskyttelsesrådgiver får overdraget andre oppgaver eller plikter, *der medfører, at vedkommende kan fastlægge formålene med og hjælpemidlerne til behandlingen af personoplysninger* hos den dataansvarlige eller databehandleren, hvilket det tilkommer den nationale retsinstans at afgøre *fra sag til sag på grundlag af en vurdering af alle relevante omstændigheder*, navnlig den dataansvarliges eller databehandlerens organisatoriske struktur og i lyset af alle gældende regler, *herunder disse sidstnævntes eventuelle interne regler*» (vår kursiv).¹⁶⁸

¹⁶³ DPO - Functional Job Description - Group Legal - Associate Lawyer & DPO – Excel.

¹⁶⁴ DPO - Functional Job Description - Group Legal - Associate Lawyer & DPO – Excel.

¹⁶⁵ Personvernforordningen artikkel 39 nr. 1 bokstav a lyder som følger: «informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til denne forordning, og i henhold til andre av Unionens eller medlemsstatenes bestemmelser om vern av personopplysninger».

¹⁶⁶ Det vil være ulike vurderinger for en intern advokat og en ekstern advokat som er innleid som personvernombud. For en ekstern advokat kan det være tydeligere skiller mellom de enkelte klienter og oppgaver (selv om det også her kan oppstå bindinger som utfordrer uavhengigheten), mens det for en intern advokat som rådgir om personvern i virksomheten kan være vanskeligere å holde adskilt rådgivningen og deretter den mer objektive rollen som ombud hvor hensynet til de registrerte skal vektlegges framfor virksomhetens interesser.

¹⁶⁷ EU-domstolen sak C-453/21 *X-FAB Dresden v FC*, avsnitt 46.

¹⁶⁸ Ibid. Telenor har i tilsvaret sitert den engelske språkversjonen av dommen, mens vi viser til den danske språkversjonen.

Vi mener at i denne avgjørelsen kommer EU-domstolen med *eksempler* på omstendigheter som kan innebære at personvernombudet har en interessekonflikt. Det som er viktig her er at det beror på en konkret vurdering i hver enkel sak hva som utgjør en interessekonflikt og om personvernombudet anses som uavhengig. Videre vektlegger vi at EU-domstolen peker spesifikt på interne retningslinjer i denne vurderingen, noe som er mangelfullt i denne saken.

Domstolens uttalelse som Telenor ASA viser til må også leses i sammenheng med avsnitt 40 i samme dom:

«Det følger således for det første af denne bestemmelses ordlyd, at databeskyttelsesforordningen ikke fastslår, at der principielt er uforenelighed mellem på den ene side udøvelsen af databeskyttelsesrådgiverens funktioner og på den anden side udøvelsen af *andre funktioner* hos den dataansvarlige eller databehandleren. Databeskyttelsesforordningens artikel 38, stk. 6, fastsætter nemlig specifikt, at databeskyttelsesrådgiveren kan overdrages udførelsen af *andre opgaver og pligter* end dem, der påhviler denne i henhold til denne forordnings artikel 39.» (vår kursiv)

Domstolen viser her til at personvernombudet kan utføre andre oppgaver enn dem som ombudet utfører etter artikkel 39. Videre skal det «ikke overdrages udførelsen af opgaver eller pligter, der kan skade udøvelsen af de funktioner, som vedkommende udøver som databeskyttelsesrådgiver».¹⁶⁹

Det må derfor være et klart skille mellom oppgaver som ombudet utfører i kraft av sin rolle som ombud og andre oppgaver. Et slikt skille vil være uklart eller umulig dersom ombudet utfører tilsvarende oppgaver eller oppgaver som et ombud skal føre kontroll med. Vi viser her til oppgavebeskrivelsen gjengitt over som viser oppgaver som langt på vei er utførende personvernoppgaver, og hvor ombudet har en rådgivende eller kontrollerende funksjon.

Uklarheten med hensyn til oppgavene som utføres som henholdsvis personvernombud og advokatfullmektig forsterkes av at det i tilsynsperioden ikke er noe som tyder på at Telenor ASAs personvernombud brukte en egen postkasse for personvernombudssaker.¹⁷⁰ Videre oppgir personvernombudets e-postsignatur begge hennes roller som følger:

¹⁶⁹ EU-domstolen sak C-453/21 *X-FAB Dresden v FC*, avsnitt 41

¹⁷⁰ Vi bemerker e-postadressen «tnasa_dpo@telenor.com» i Telenor ASAs personvernerklæring oppdatert 3. februar 2022, men Telenor ASA har ikke forelagt oss noe dokumentasjon på at denne e-postadressen eksisterte eller ble brukt i tilsynsperioden.

N.N.

Associate Lawyer and Data Protection Officer (DPO) Telenor ASA
Group Legal

Telenor Group
+47 xxxxxxxx
Snarøyveien 30
N-1360 Fornebu
www.telenor.com

[Facebook](#) | [Twitter](#) | [LinkedIn](#)



Det vil derfor ikke være mulig for en kollega som mottar e-post fra henne med råd om personvern, å vite om rådene gis i egenskap av rollen som personvernombud eller juridisk rådgiver.

En prinsipal har etter norsk lov plikt til å gi fullmektigen veiledning,¹⁷¹ og fullmektigen har plikt til å holde prinsipalen orientert om arbeidet som utføres.¹⁷²

Telenor ASA skriver i sine merknader til varsel:

«Prinsipal–fullmektig-relasjonen gjelder ikke rollen som personvernombud. Synspunktet forutsetter derfor at prinsipalen som advokat vil handle i strid med kravet til uavhengighet. Dette er en ren teoretisk risiko, og den gjør seg gjeldende ved alle over- og underordningsforhold, ikke kun en prinsipal–fullmektig-relasjon. Derimot må det legges til grunn at en overordnet som er advokat, har et særlig bevisst forhold til rolleforståelse og uavhengighet, og at risikoen derfor er mindre enn ellers for at uavhengigheten skal bli påvirket.»

Vi bemerker at lederen av et juridisk team normalt er den som (i det minste delvis) bestemmer formålet med behandlingen av personopplysninger som utføres av teamet i forbindelse med utførelsen av oppgavene som er tildelt teamet (f.eks. hvilke personopplysninger som behandles i forbindelse med juridiske prosesser.) Det er mulig at prinsipal–fullmektig–forholdet vil påvirke utførelsen av personvernombudets oppgaver med hensyn til behandlingsaktiviteter som utføres eller på annen måte påvirkes av prinsipalens arbeid, da det kan være vanskelig for en advokatfullmektig å ta til motmæle mot sin prinsipal. Selv om prinsipal–fullmektig–relasjonen bare gjelder for advokatfullmektigrollen, vurderer vi at det er risiko for at vedkommende kan bli mer opptatt av å oppnå advokatbevilgning enn utførelse av

¹⁷¹ Forskrift til domstolloven (Advokatforskriften) Til kapittel 12. Regler for god advokatskikk, punkt 5.6 og 5.7.

¹⁷² Se Den norske advokatforening («Advokatforeningen, Veiledning for prinsipal og advokatfullmektig» (22. november 2019)).

sine oppgaver som personvernombud. Alle risikoer inkludert teoretiske må vurderes konkret for å avgjøre personvernombudets uavhengighet og om det finnes interessekonflikt. Disse vurderingene bør dokumenteres som en del av internkontrollen jf. personvernforordningen artikkel 24 nr. 1.

For å kunne utføre sine oppgaver på en skikkelig måte er det ofte slik at personvernombudet må innta en konsekvent, insisterende holdning, også overfor ansatte som har en overordnet posisjon og beslutningsmakt i organisasjonen, noe som i beste fall kan oppfattes som byråkratisk og i verste fall som et ubehagelig uromoment. Personvernombudet må dermed være i en posisjon til å håndtere presset og vanskelighetene som følger med denne viktige posisjonen.¹⁷³

At budsjettet for personvernrelaterte utgifter i Telenor ASA «[is] allocated on a case-by-case basis by line management»¹⁷⁴ svekker personvernombudets posisjon ytterligere. Et personvernombud som må be sin overordnede om ressurser kan møte på vanskeligheter, særlig hvis sistnevnte ikke er fast forpliktet til overholdelse av krav til personvern.¹⁷⁵ I denne saken har ikke Telenor ASAs personvernombud en egen budsjettpost og må søke om midler til personvernarbeid fra sin linjeleder, som også er en av personvernombudets prinsipaler. Dette kan ha negative konsekvenser for personvernombudets uavhengighet.

Til slutt ble det under tilsynet klart at alle personvernombud i Telenor-konsernet, herunder personvernombudet i Telenor ASA, eier aksjer i selskapet.¹⁷⁶ Telenor ASA har verken vurdert om dette kan føre til interessekonflikter for personvernombudene eller utarbeidet interne regler for å hindre mulige interessekonflikter for personvernombud i egenskap av aksjonærer. Det er en kjent problemstilling at for enkelte yrker som krever en høy grad av uavhengighet (f.eks. advokater), kan det å eie aksjer i et selskap være uforenlig med kravet om uavhengighet. Særlig gjelder dette dersom aksjonæren som er underlagt et slikt krav utfører aktiviteter som kan ha innvirkning på aksjeverdien.¹⁷⁷ Dette er tilfellet for mange av oppgavene til et personvernombud der rådene vedkommende gir, hvis de følges, kan føre til betydelige endringer i selskapets forretningsmodell. Å være aksjonær i selskapet kan således føre til interessekonflikter for et personvernombud, særlig hvis det ikke er noen grenser for hvor mange aksjer vedkommende kan erverve. Dette kan i sin tur påvirke personvernombudets uavhengighet når vedkommende blir bedt om å gi råd om særlig forretningskritiske behandlingsaktiviteter. Som Telenor ASA påpeker i tilsvaret er det snakk om et lavt antall aksjer. Det er ikke noen automatikk i at aksjeeierskap fører til interessekonflikt, men dette er et spørsmål som Telenor ASA burde ha vurdert og dokumentert.

¹⁷³ Se Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (14. oktober 2010), s. 6.

¹⁷⁴ «Response to Datatilsynet additional documentation», 10.01.2022, s. 4.

¹⁷⁵ Se Network of Data Protection Officers of the EU Institutions and Bodies, Professional Standards for Data Protection Officers of the EU institutions and bodies working under Regulation (EC) 45/2001 (14. oktober 2010), s. 6.

¹⁷⁶ Endelig tilsynsrapport av 30. september 2022, s. 25.

¹⁷⁷ Se <https://www.advokatforeningen.no/advokatetikk/regler-og-retningslinjer/uttalelser-fra-etikkutvalget/10-betaling-for-advokatbistand-med-aksjer/>

Vi har ikke vurdert det eksterne personvernombudets uavhengighet og mulige interessekonflikter, men merker oss at han var innleid som ekstern konsulent i en begrenset periode. Hans grad av uavhengighet var dermed strukturelt forskjellig fra personvernombudet på tilsynstidspunktet som var fast ansatt i stilling som både personvernombud og advokatfullmektig.

Vi bemerker for øvrig at i de 6 månedene av tilsynsperioden som personvernombudet hadde to roller, jobbet hun i utgangspunktet 100 prosent med personvernombudsoppgaver, i den grad personvernombudsoppgavene var mulig å skille fra advokatfullmektigoppgavene (noe Datatilsynet mener at de ikke alltid var). Dermed var risikoen for at interessekonflikter skulle materialisere seg mindre i praksis. Samtidig er det enkelte av omstendighetene ovenfor som uansett utfordrer uavhengigheten, for eksempel hva gjelder avhengighetsforholdet for å få prøvesaker og advokatbevilgning. Slike avhengighetsforhold kan under enkelte omstendigheter gi uheldige utslag, for eksempel hvis et personvernombud velger å prioritere ned å involvere seg i krevende saker som gjør at vedkommende fremstår «vanskelig», av hensyn til videre karriereutvikling. Datatilsynet er i tvil om rollen som intern advokatfullmektig i det hele tatt lar seg kombinere med rollen som personvernombud.

Datatilsynet har ikke nok informasjon til å konkludere på dette punktet. Uansett finner vi at Telenor ASA ikke har gjennomført alle vurderinger de burde og at det manglet tydeligere skille mellom rollene og oppgaver som personvernombud og advokatfullmektig. Se punkt 12.2 om kravene i personvernforordningen artikkel 24 nr. 1 og 2.

11 Personvernombudets oppgaver, artikkel 39 nr. 1

11.1 Tilsynskriterier og tilsynsbevis

Personvernforordningen artikkel 39 første og andre punktum lyder som følger:

1. Personvernombudet skal minst ha følgende oppgaver:
 - a) informere og gi råd til den behandlingsansvarlige eller databehandleren og de ansatte som utfører behandlingen, om de forpliktelsene de har i henhold til denne forordning, og i henhold til andre av Unionens eller medlemsstatenes bestemmelser om vern av personopplysninger,
 - b) kontrollere overholdelsen av denne forordning, av andre av Unionens eller medlemsstatenes personvernregler og den behandlingsansvarliges eller databehandlerens personvernretningslinjer, herunder fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som er involvert i behandlingsaktivitetene, og tilhørende revisjoner,
 - c) på anmodning gi råd om vurderingen av personvernkonsekvenser og kontrollere gjennomføringen av den i henhold til artikkel 35,
 - d) samarbeide med tilsynsmyndigheten,

- e) fungere som kontaktpunkt for tilsynsmyndigheten ved spørsmål om behandlingen, herunder forhåndsdrøftingene nevnt i artikkel 36, og ved behov rådføre seg med tilsynsmyndigheten om eventuelle andre spørsmål.
2. Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i.

Vi viser videre til punkt 3.8.1 og 3.8.2 i den endelige tilsynsrapporten av 30. september 2022.

11.2 Datatilsynets vurdering

Samlet sett gjenspeiles oppgavene i personvernforordningen artikkel 39 nr. 1 i stillingsbeskrivelsen til Telenor ASAs personvernombud, konsernhåndboken i personvern fra 2020¹⁷⁸ og konsernhåndboken i personvern fra 2022.¹⁷⁹ Selv om vi mener at beskrivelsen av personvernombudets oppgaver burde være mer spesifikk, for eksempel når det gjelder hvordan og når personvernombudet bør involveres i håndteringen av brudd på personopplysningssikkerheten og vurderingen av personvernkonsekvenser, konkluderer vi ikke med overtredelse av personvernforordningen artikkel 39 nr. 1 innenfor tilsynsperioden, da det ikke foreligger tilstrekkelig sannsynlighetsovervekt.

12 Organisatoriske tiltak for å sikre overholdelse av artikkel 24 nr. 1 og 2

12.1 Tilsynskriterier og tilsynsbevis

Personvernforordningen artikkel 24 nr. 1 og 2 lyder som følger:

1. Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.
2. Dersom det står i et rimelig forhold til behandlingsaktivitetene, skal tiltakene nevnt i nr. 1 omfatte den behandlingsansvarliges iverksetting av egnede retningslinjer for vern av personopplysninger.

Vi viser til punkt 3.9.1 og 3.9.2 i den endelige tilsynsrapporten av 30. september 2022.

12.2 Datatilsynets vurdering

Personvernforordningen artikkel 24 nr. 1 fastsetter at den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen

¹⁷⁸ «Group Manual Privacy, Valid from: 01.06.2020», punkt 2.2.2.

¹⁷⁹ «Group Manual Privacy, Valid from: 2022-01-01», punkt 1.1.

utføres i samsvar med personvernforordningen. Nevnte tiltak bør ta hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene for fysiske personers rettigheter og friheter.

12.2.1 Omfanget av behandlingsansvar

Behandlingen som utføres av Telenor ASA omfatter ulike kategorier av personopplysninger.¹⁸⁰ På bakgrunn av Telenor ASAs artikkel 30-protokoll ser det ut til at en begrenset mengde personopplysninger som behandles av Telenor ASA, faller inn under definisjonen av særlige kategorier av personopplysninger, jf. personvernforordningen artikkel 9 nr. 1.¹⁸¹ Telenor ASA behandler for det meste personopplysninger knyttet til egne ansatte (ca. 380), men også om andre ansatte i Telenor Group (ca. 15 000 totalt¹⁸²), samt kunder og andre enkeltpersoner.¹⁸³ Selv om Telenor ASA ikke har direkte kundeforhold, behandler Telenor ASA kundeopplysninger som opprinnelig ble samlet inn av dets datterselskaper innenfor «Group Unit Internal Audit & Investigations» (GIAI) og «Telenor Research».¹⁸⁴ Telenor ASA behandler også personopplysninger som opprinnelig stammer fra datterselskapene i sin daglige kontroll med deres etterlevelse av konsernets retningslinjer i Compliance-avdelingen.¹⁸⁵

Behandlingsaktiviteter som utføres av Telenor ASAs datterselskaper, er kun relevante for denne saken i den grad Telenor ASA regnes som behandlingsansvarlig, enten alene eller i fellesskap med det aktuelle datterselskapet, eller der Telenor ASA regnes som databehandler og/eller det aktuelle datterselskapet opptrer som databehandler eller underdatabehandler for Telenor ASA.

Det ligger utenfor dette tilsynets rammer å trekke konklusjoner om Telenor ASAs rolle i alle de ulike behandlingsaktivitetene som utføres i selskapet og dets datterselskaper. Å se overordnet på relevante fakta i saken kan imidlertid si noe om i hvilke forpliktelser som påhviler Telenor ASA.

Telenor ASAs rolle i de ulike behandlingsaktivitetene har konsekvenser for selskapets ansvar. For eksempel skal en databehandler bare behandle personopplysninger på dokumenterte instruksjoner fra den behandlingsansvarlige i henhold til personvernforordningen artikkel 28 nr. 3 bokstav a. En behandlingsansvarlig er derimot ansvarlig for og må kunne påvise at prinsippene for behandling av personopplysninger overholdes etter personvernforordningen artikkel 5 nr. 2. Dessuten retter artikkel 24 seg som nevnt mot den behandlingsansvarlige.

Overfor sine datterselskaper opptrer Telenor ASA både som behandlingsansvarlig, felles behandlingsansvarlig og databehandler.¹⁸⁶ Telenor ASAs rolle skal vurderes i hver enkelt

¹⁸⁰ Endelig tilsynsrapport av 30. september 2022, s. 4–5.

¹⁸¹ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

¹⁸² Endelig tilsynsrapport av 30. september 2022, s. 10.

¹⁸³ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

¹⁸⁴ Endelig tilsynsrapport av 30. september 2022, s. 4–5.

¹⁸⁵ Endelig tilsynsrapport av 30. september 2022, s. 4–7 og 10.

¹⁸⁶ Endelig tilsynsrapport av 30. september 2022, s. 6.

situasjon. Behandlingsansvaret ligger hos selskapet eller selskapene som, alene eller sammen med andre, bestemmer formålene med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. personvernforordningen artikkel 4 nr. 7. Et av hovedelementene i den forbindelse er hvem som utøver avgjørende innflytelse over behandlingen for egne formål.¹⁸⁷ En behandlingsansvarlig kan for eksempel utøve innflytelse over behandlingen av personopplysninger for å oppfylle sine rettslige forpliktelser.¹⁸⁸ Når et selskap i Telenor Group behandler personopplysninger på vegne av den behandlingsansvarlige, regnes det som databehandler i henhold til personvernforordningen artikkel 4 nr. 8.

Telenor ASA fastholder at de andre selskapene i Telenor Group fungerer som separate behandlingsansvarlige for sine egne behandlingsaktiviteter, og for behandlingsaktiviteter som Telenor ASA utfører med personopplysninger som opprinnelig ble samlet inn av de andre selskapene.¹⁸⁹ Særlig i forbindelse med behandling av kundeopplysninger fastholder Telenor ASA at de opptrer som databehandler på vegne av datterselskapene.¹⁹⁰ Ifølge artikkel 30-protokollen er imidlertid Telenor ASA å anse som behandlingsansvarlig, f.eks. for behandling av personopplysninger om ansatte i Telenor Group for behandlingsaktivitetene «Corporate Social Networking» og «Learning Management Systems». Det er uansett de faktiske omstendighetene som er avgjørende for vurderingen om hvem som er behandlingsansvarlig.¹⁹¹ Dersom Telenor ASA i en bestemt sammenheng utøver innflytelse over behandlingen i den forstand at Telenor ASA alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger i sine datterselskaper og hvilke midler som skal benyttes, vil Telenor ASA være (felles) behandlingsansvarlig for behandlingen.

EU-domstolen har fastslått at begrepet «behandlingsansvarlig» må defineres bredt, og at:

«fælles ansvar ikke nødvendigvis, at forskjellige aktører har samme ansvar for den samme behandling af personopplysninger. De forskellige aktører kan tværtimod være ansvarlige for behandlingen af personopplysninger på forskjellige niveauer og i forskelligt omfang, således at den enkeltes ansvarsniveau skal vurderes under hensyntagen til samtlige relevante omstændigheder i saken».¹⁹²

Videre betyr felles ansvar blant flere aktører «ikke, at hver af disse har adgang til de omhandlede personopplysninger».¹⁹³

¹⁸⁷ EU-domstolen sak C-25/17, *Jehovas vitner*, ECLI:EU:C:2018:551, avsnitt 68.

¹⁸⁸ EDPB, Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse Version 2.0 (vedtatt 7. juli 2021), s. 13.

¹⁸⁹ Endelig tilsynsrapport av 30. september 2022, s. 3–8 og 10.

¹⁹⁰ Endelig tilsynsrapport av 30. september 2022, s. 3–4, 5 og 8.

¹⁹¹ EDPB Retningslinjer 07/2020 for begreberne dataansvarlig og databehandler i den generelle forordning om databeskyttelse Version 2.0, s. 13.

¹⁹² EU-domstolen sak C-25/17, *Jehovas vitner*, ECLI:EU:C:2018:551, avsnitt 66. Se også sak C-210/16 *Wirtschaftsakademie* EU:C:2018:388, avsnitt 28, 43 og 44.

¹⁹³ EU-domstolen sak C-25/17, *Jehovas vitner*, ECLI:EU:C:2018:551, avsnitt 69 og sak C-210/16 *Wirtschaftsakademie* EU:C:2018:388, avsnitt 38.

Telenor ASA behandler kundeopplysninger blant annet i forbindelse med undersøkelser i Telenor Groups markeder for det formål å forstå kundeatferd.¹⁹⁴ Det dreier seg om flerårige spørreundersøkelser i flere land, med både forretnings- og forskningsformål.¹⁹⁵ Telenor ASA definerer seg selv som databehandler for denne spesifikke behandlingsaktiviteten.¹⁹⁶ At disse undersøkelsene gjennomføres i stor skala i hele Telenor Group, og at de omfatter ulike markeder i Telenor Group med det formål å forstå kundeatferd i disse markedene, tyder på at det ikke bare er Telenor ASAs datterselskaper som skal anses som behandlingsansvarlige for denne behandlingen. Det virker lite sannsynlig at Telenor ASA ikke, i alle fall til en viss grad, utøver innflytelse over formålet med og midlene for denne behandlingen. Datatilsynet anser at dette kan være en behandlingsaktivitet som Telenor ASA har et felles behandlingsansvar for med sine datterselskaper.

Det er dessuten flere situasjoner der datterselskapene gis ansvar for å iverksette instruksjoner, f.eks. gjennom konsernets styrende dokumenter.¹⁹⁷ I enkelte tilfeller setter disse dokumentene rammer for datterselskapenes aktivitet, herunder hva gjelder behandling av personopplysninger. I lys av dette anser Datatilsynet at Telenor ASA kan fungere som felles behandlingsansvarlig sammen med sine datterselskaper for noen av behandlingsaktivitetene som utføres i Telenor Group. Vi konkluderer imidlertid ikke på dette punktet; dette må Telenor ASA vurdere.

Det eksterne personvernombudet beskrev situasjonen slik:

«[...] as long as ASA has an operational involvement in business activities involving processing of personal data, whether it's within ASA itself or exercised upon other businesses through ASAs role as HQ, there are privacy obligations to adhere to that ASA cannot fully escape.»¹⁹⁸

Som nevnt ligger det utenfor dette tilsynets rammer å med sikkerhet konkludere angående Telenor ASAs rolle i de ulike behandlingsaktivitetene i Telenor Group. Slik avklaring vil være en oppgave som et personvernombud, med sin personvernekspertise og kjennskap til virksomheten, bør involveres i.

I denne saken legger vi kun til grunn det Telenor ASA selv har skrevet i behandlingsprotokollen, i den grad det bare er krav om alminnelig sannsynlighetsovervekt.

På bakgrunn av de innhentede tilsynsbevisene oppfatter vi at det i flere tilfeller er uklart når Telenor ASA regnes som behandlingsansvarlig, felles behandlingsansvarlig eller databehandler for spesifikke behandlingsaktiviteter. Det gjelder både for behandling i andre selskaper i Telenor Group og i Telenor ASA i tilknytning til opplysninger som opprinnelig ble samlet inn av andre selskaper i konsernet. Vi finner det imidlertid sannsynliggjort at Telenor

¹⁹⁴ Endelig tilsynsrapport av 30. september 2022, s. 5.

¹⁹⁵ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

¹⁹⁶ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

¹⁹⁷ Endelig tilsynsrapport av 30. september 2022, s. 6.

¹⁹⁸ Endelig tilsynsrapport av 30. september 2022, s. 9.

ASA er behandlingsansvarlig for mer enn det selskapet selv har lagt til grunn i sine svar til Datatilsynet.

12.2.2 Angående organisatoriske tiltak

I denne delen vurderer vi de organisatoriske tiltakene Telenor ASA hadde knyttet til artikkel 38 og for generell overholdelse av personvernforordningen.

I henhold til ansvarlighetsprinsippet i personvernforordningen artikkel 5 nr. 2 skal Telenor ASA kunne påvise at behandlingen skjer i samsvar med de øvrige personvernprinsippene. Det følger av artikkel 24 nr. 1 at den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med forordningen.

I henhold til artikkel 24 nr. 2 skal den behandlingsansvarlige iverksette egnede retningslinjer for vern av personopplysninger dersom det står i et rimelig forhold til behandlingsaktivitetene. Dette betyr at de organisatoriske tiltakene bør omfatte interne retningslinjer for personvern der det anses som relevant og forholdsmessig.

Telenor ASA er i alle fall behandlingsansvarlig for en rekke behandlinger av ansattopplysninger. For denne typen behandlingsaktiviteter, som skjer i en profesjonalisert sammenheng og i kontekst av et stort konsern, er det åpenbart rimelig å forvente i alle fall grunnleggende retningslinjer og et minimumsnivå av internkontroll for etterlevelse av personvernforordningen. Noe annet ville undergravd formålet med artikkel 24 og ansvarlighetsprinsippet.

Vi bemerker at ytterligere behandlingsaktiviteter der Telenor ASA identifiseres som behandlingsansvarlig alene eller felles, kan stille enda strengere krav til hvilke retningslinjer som må være på plass.

For ordens skyld presiserer vi at organisatoriske tiltak, dokumentasjon og retningslinjer må konkretisere *hvordan* virksomheten skal følge personvernforordningen. Det er selvsagt ikke tilstrekkelig å bare gjenta eller henvise til lovens ordlyd.

Telenor ASA må altså vedta skriftlige retningslinjer, med klart og presist innhold, som skissert nedenfor. De dokumenterte retningslinjene bør gi detaljerte beskrivelser som Telenor ASA kan henvise til og bruke internt når det gjelder personvernombudsordningen.

I tilsvaret viser Telenor ASA til at det avgjørende er om tiltak har effekt.¹⁹⁹ Det er uansett Telenor ASA sitt ansvar å sørge for å formalisere og dokumentere retningslinjene, slik at etterlevelse kan påvises, og å utarbeide retningslinjene på en slik måte at de er operasjonaliserbare og dermed har effekt.

¹⁹⁹ Ibid.

For det første viser vi til punkt 6.2 over, der vi konkluderte med at det var en risiko for at Telenor ASAs personvernombud ikke involveres i alle spørsmål som gjelder vern av personopplysninger, på riktig måte og i rett tid. Vi ble ikke forelagt noen retningslinjer som viste og sørget for involvering av personvernombudet i Telenor ASA. Av den grunn har det vært vanskelig å ta stilling til om vilkåret i personvernforordningen artikkel 38. nr. 1 var oppfylt eller ikke. Vi har latt tvilen komme selskapet til gode.

Telenor ASA mener at det ikke er grunnlag for å kreve formaliserte retningslinjer siden vi valgte å ikke konstatere brudd på personvernforordningen artikkel 38. nr. 1.²⁰⁰ At fraværet av retningslinjer har gjort det vanskelig for Datatilsynet å konkludere om spørsmålene, kan ikke forstås slik at det dermed ikke foreligger brudd. Vi vurderer at mangel på retningslinjer er et selvstendig brudd på personvernforordningen artikkel 24, og mener det er behov for vurderinger og dokumentasjon på disse som en del av internkontrollen.

Datatilsynet finner at beskrivelsen av *når og på hvilken måte* personvernombudet skal involveres, er utilstrekkelig. Telenor ASA har ikke forelagt oss noen skriftlige rutiner eller andre egnede retningslinjer for når og på hvilken måte Telenor ASAs personvernombud skal involveres i alle spørsmål som gjelder vern av personopplysninger inkludert DPIA og avvikshåndtering. Tilsynet har avdekket at personvernombudets involvering i personvernspørsmål generelt har vært uformell, og i stor grad blitt avgjort fra sak til sak. Vi mener derfor at Telenor ASA ikke hadde etablert organisatoriske tiltak for å sikre og påvise at alle behandlingsaktiviteter ble utført i samsvar med personvernforordningen, og ikke hadde innført tilstrekkelig interne retningslinjer for når og hvordan personvernombudet skulle involveres i alle personvernspørsmål.

For det andre viser vi til punkt 8.2 over,²⁰¹ hvor vår vurdering er at Telenor ASA ikke har klart å påvise at det i tilsynsperioden var etablert organisatoriske tiltak i form av en formalisert rapporteringslinje mellom personvernombudet og øverste ledelsesnivå²⁰² i Telenor ASA. Problemstillingen ble tatt opp av det eksterne personvernombudet.²⁰³ Telenor ASA har ikke forelagt oss noen offisielle skriftlige retningslinjer som beskriver og sikrer personvernombudets tilgang til øverste ledelsesnivå. Som diskusjonen under 8.2 viser, er det helt sentralt at selskapet vurderer hvordan og til hvem rapporteringen skal skje i praksis og konkretiserer og dokumenterer dette i klare og entydige retningslinjer. Dette har manglet i Telenor ASA.

Vi mener i denne saken, å nevne personvernombudets mulighet til å rapportere direkte til «CEO 1. escalation» og «BoD 2. escalation» (Board of Directors/styret)²⁰⁴ i PowerPoint-presentasjoner, ikke er tilstrekkelig.

²⁰⁰ Merknader til forhåndsvarsel av 31. mai 2024, s. 47-48

²⁰¹ Punkt 8.2.

²⁰² Jf. personvernforordningen artikkel 5 nr. 2 og artikkel 24.

²⁰³ «2021.09.09 – TNASA Privacy status and proposals for GU Forum», s. 13. Punkt 8.2.

²⁰⁴ «TNASA Privacy organisation overview, per 2021.12.06 and 2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf»

For øvrig merker vi oss at de nye, oppdaterte retningslinjene – Group Manual Privacy og Group Policy Privacy – gyldig fra 1. januar 2022, heller ikke nevner rapporteringslinjen til styret. Følgende setning fra Group Manual Privacy (gyldig mellom 1. juni og 31. desember 2021) var til og med fjernet i den oppdaterte versjonen som trådte i kraft 1. januar 2022:

«The DPO shall have the right to report all privacy-related incidents and non-conformities directly to the BU CEO»²⁰⁵

I dette tilfellet har vi sett ulike tolkninger i Telenor ASAs dokumentasjon av hva som skal anses som øverste ledelse. Vi er av den oppfatning at det i interne retningslinjer for selskapet må fremgå tydelig hva som er øverste ledelsesnivået i Telenor ASA, samt en beskrivelse av hvordan personvernombudet er sikret direkte rapporteringslinje dit.

Telenor ASAs beslutninger om å bruke CCM og GU Forum som rapporteringsarenaer og de nevnte endringene i tidligere håndbøker og retningslinjer viser i hovedsak hvor uklart innholdet i de interne retningslinjene har vært. Selv om det ville være mulig for et personvernombud å ha uformell kontakt med styret og den daglige toppledelsen, ville det mest sannsynlig være avhengig av personlig bekjentskap og kanskje tilfeldigheter. Uansett må selskapene ha etablert egnede organisatoriske tiltak, herunder retningslinjer, som under alle omstendigheter er pålitelige og tilgjengelige, for å kunne sikre og påvise overholdelse.

For det tredje viser vi til punkt 10.2 over, der Datatilsynet ikke hadde tilstrekkelig informasjon til å konkludere om personvernombudet var sikret tilstrekkelig uavhengighet og om fravær av interessekonflikt. Her burde det ha blitt gjort en konkret og dokumentert analyse av mulige risikoer. Som tidligere nevnt finner vi at de organisatoriske tiltakene Telenor ASA har iverksatt, ikke sikrer et tydelig skille mellom de oppgavene som skal utføres som henholdsvis personvernombud og advokatfullmektig. Her er det flere organisatoriske tiltak som hadde vært egnet, alt fra plassering i organisasjonen for å unngå avhengighetsforhold til at personvernombudet måtte bruke en separat e-post-adresse for å tydeliggjøre skillet mellom roller. Telenor ASA har i tillegg verken vurdert om det at personvernombudet eier aksjer i selskapet kan føre til interessekonflikter eller iverksatt organisatoriske tiltak for å hindre mulige interessekonflikter for personvernombud/aksjonærer. Vi mener at Telenor ASAs gjennomføring av organisatoriske tiltak i den forbindelse har vært mangelfull. Vi mener at disse tiltakene ikke oppfyller de rettslige kravene i personvernforordningen artikkel 24 nr. 1. Uansett er ikke Telenor ASA i stand til å påvise etterlevelse med personvernforordningens regler.

For det fjerde viser vi til vår vurdering i punkt 8.2, der vi siterer direkte fra den tidligere «Group Manual Privacy», som slo fast at «GPO shall act as DPO in Telenor ASA».²⁰⁶ Telenor ASA bemerket i sine kommentarer til tilsynsrapporten at «DPO» i den forbindelse var ment å vise til at personvernombudet på det tidspunktet var organisert under «Group Privacy & IM», ikke «Group Legal».²⁰⁷ Telenor ASA gjør også gjeldende at personvernombudets ansvar og oppgaver ikke er presentert i «Group Manual Privacy», da den

²⁰⁵ «Group Manual Privacy, valid from 1 June 2020», s. 5.

²⁰⁶ «Group Manual Privacy, valid from: 01.06.2020», s. 3–4.

²⁰⁷ Foreløpig tilsynsrapport med merknader fra Telenor ASA i gult, 16. mai 2022, s. 12.

gjelder Telenor som konsern.²⁰⁸ Telenor ASA understreket at «GPO» og «DPO» alltid har vært to atskilte roller.²⁰⁹ Datatilsynet bemerker at Telenor ASA har holdt oss oppdatert om hvem som har hatt rollen som personvernombud i Telenor ASA, og at det var ████████ som var GPO da noen andre hadde rollen som DPO. Dette viser at Telenor ASAs praksis avviker fra det som sto i konsernets interne retningslinjer. Telenor har erkjent at «they understand that the text is imprecise and can be misunderstood».²¹⁰ Det er vanskelig å forstå hvorfor det står i retningslinjene at GPO skal fungere som personvernombud i Telenor ASA når dette ikke er tilfellet.

Telenor ASA skriver blant annet i merknader til varsel:

«Det er ikke utdypet eller angitt hvilke tiltak Datatilsynet mener er nødvendig på bakgrunn av Group Privacy Manual. I den grad Datatilsynet mener at ordlyden i disse retningslinjene må justeres, vil Telenor på nytt understreke at forholdet ikke utgjør et selvstendig brudd på GDPR artikkel 24. nr. 1 og 2. En slik endring vil ikke ha en faktisk effekt hva gjelder personvernombudets stilling i Telenor ASA»

Videre stiller Telenor ASA spørsmål om personvernforordningen artikkel 24. nr. 1 og 2 på et selvstendig grunnlag gir hjemmel for særskilte retningslinjer om personvernombudet. Telenor ASA hevder at «internkontrollbestemmelsen i GDPR artikkel 24. nr. 1 og 2 retter seg mot "behandlingen", og skal sikre at behandlingen av personopplysninger er i overensstemmelse med kravene i GDPR.»²¹¹ Deres tolking er dermed at personvernforordningen artikkel 24 kun gjelder den enkelte behandlingsaktivitet, og ikke gjelder generelt. Dette er imidlertid en snever forståelse av bestemmelsen som vi ikke er enige i.

Det følger av flere rettskilder at personvernforordningen artikkel 24 er en internkontrollbestemmelse, slik Telenor ASA også skriver, og at den gjelder etterlevelse av forordningen generelt. Fortalepunkt 78 slår fast at det kreves «at det treffes egnede tekniske og organisatoriske tiltak for å sikre at kravene i denne forordning oppfylles». Med andre ord er formålet og lovgivernes intensjon at kravet om egnede tekniske og organisatoriske tiltak for å sikre etterlevelse gjelder generelt og ikke bare «behandlingen».

Både Jarbekk m.fl. og Skullerud m.fl. omtaler personvernforordningen artikkel 24 som interkontroll og at bestemmelsen i stor grad viderefører internkontrollbestemmelsen fra tidligere personopplysningsloven (2000) § 14.²¹² Jarbekk m.fl. skriver at «den behandlingsansvarlige s[kal] gjennomføre «egne tekniske og organisatoriske tiltak» for «å sikre og påvise» etterlevelse av forordningen» (vår understreking).²¹³

²⁰⁸ Foreløpig tilsynsrapport med merknader fra Telenor ASA i gult, 16. mai 2022, s. 12.

²⁰⁹ Foreløpig tilsynsrapport med merknader fra Telenor ASA i gult, 16. mai 2022, s. 12.

²¹⁰ Foreløpig tilsynsrapport med merknader fra Telenor ASA i gult, 16. mai 2022, s. 12.

²¹¹ Merknader til forhåndsvarsel 31. mai 2024, s. 49.

²¹² Eva Jarbekk mfl.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019), s 256. Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave* (2019) s. 273.

²¹³ Eva Jarbekk mfl.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019), s 256.

Det er dermed en bestemmelse som fastslår det som egentlig er opplagt, nemlig at behandlingsansvarlig har en plikt til å etterleve alle relevante bestemmelser i forordningen. Personvernforordningen artikkel 24 må tolkes i lys av personvernforordningen artikkel 5 nr. 2 og ansvarlighetsprinsippet, og må leses som en bestemmelse om «accountability».²¹⁴ Bestemmelsen ble innført som en konsekvens av at det tidligere personverndirektivets ordning med meldeplikt til datatilsynene forsvant.²¹⁵ Ansvar for etterlevelse legges dermed fullt ut til behandlingsansvarlig.²¹⁶

Det ville videre vært direkte i strid med bestemmelsens formål og sammenheng, jf. de EØS-rettslige tolkningsprinsippene nevnt ovenfor, om den behandlingsansvarlige bare behøvde å iverksette tiltak for å sikre etterlevelse av enkelte bestemmelser i forordningen. Det ville i praksis ha innebåret at den behandlingsansvarlige ikke trengte å sikre etterlevelse med de andre bestemmelsene. Det er for Datatilsynet klart at lovgiver ikke har laget en slik regel.

Som Docksey påpeker så har personvernforordningen artikkel 24 utviklet seg fra personverndirektivet ved at den krever proaktiv og demonstrerbar etterlevelse:

«It places responsibility firmly on the controller to take proactive action to ensure compliance and to be ready to demonstrate that compliance. (...) Accountability in this sense requires that controllers put in place internal policies and mechanisms to ensure compliance and provide evidence to demonstrate compliance to external stakeholders, including supervisory authorities.»²¹⁷

«It is crucial for controllers to take active responsibility for ensuring compliance and develop an accountability culture at all levels of their organisation. »²¹⁸

Dokumentasjonsplikten følger av personvernforordningen artikkel 24 nr. 2. Som Skullerud m.fl. påpeker:²¹⁹

«Virksomhetens interne rutiner skal etableres og dokumenteres skriftlig.»

«Som ledd i internkontrollsystemet skal den behandlingsansvarlige implementere styrende dokumenter for ivaretagelse av personvernet til de registrerte, jf. personvernforordningen art. 24 nr. 2. Etter personopplysningsloven 2000 var det også ansett som et krav å etablere styrende dokumenter for virksomhetens behandling av personopplysninger.»

²¹⁴ Christopher Docksey, “Article 24 Responsibility of the controller” i Kuner, Bygrave og Docksey (red), *The EU General Data Protection Regulation (GDPR). A commentary*, s. 557

²¹⁵ Christopher Docksey, “Article 24 Responsibility of the controller” i Kuner, Bygrave og Docksey (red), *The EU General Data Protection Regulation (GDPR). A commentary*, s. 560

²¹⁶ Ibid

²¹⁷ Christopher Docksey, “Article 24 Responsibility of the controller” i Kuner, Bygrave og Docksey (red) *The EU General Data Protection Regulation (GDPR). A commentary* s. 555-570.

²¹⁸ Ibid s. 568

²¹⁹ Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen (GDPR), kommentarutgave (2023)*, kommentarer til artikkel 24 på nett.

Datatilsynet mener derfor at selskapets snevre forståelse av personvernforordningen artikkel 24 nr. 1 ikke kan legges til grunn.

Videre, når man har opprettet et personvernombud, er det som nevnt et krav at ombudet har uavhengighet, tilstrekkelige ressurser, direkte rapporteringslinje til høyeste ledelsesnivå, og at det involveres på bestemte måter i behandlingen. Hvis for eksempel kravene knyttet til uavhengighet ikke respekteres, kan det resultere at behandlingsaktivitetene som ombudet har vært involvert i, ikke skjer i tråd med forordningen. Tilsvarende gjelder for eksempel der et personvernombud ikke var involvert i behandlingsaktiviteter der slik involvering var påkrevd eller ikke kunne rapportere eventuelle mangler til den øverste ledelsen. Med andre ord er det en alltid en lenke – om enn indirekte – mellom konkrete behandlinger og rutiner knyttet til personvernombud. Er dokumentasjon knyttet til personvernombud mangelfull, vil det rett og slett ikke være mulig for den behandlingsansvarlige å påvise at behandlingen skjer i tråd med loven, slik bestemmelsen krever.

Av personvernforordningen artikkel 24 nr. 1 fremgår det at det at den behandlingsansvarlige skal kunne påvise etterlevelse. Feilaktige og motsigende rutiner er åpenbart ikke i tråd med dette kravet. Å ikke kunne påvise etterlevelse er altså et brudd i seg selv, uavhengig av om det kan etableres en faktisk effekt – poenget er nettopp at når dokumentasjonen ikke er tilstrekkelig, vil det ofte ikke være mulig for tilsynsmyndigheten å avdekke de faktiske forholdene.

I tilsvaret viser Telenor ASA til at artikkel 24 krever en forholdsmessighetsvurdering:

«Telenor kan ikke se at GDPR artikkel 24 nødvendiggjør retningslinjer i det omfang og detaljgrad Datatilsynet krever, når dette ikke knytter seg til selve behandlingsaktivitetene, men derimot til personvernombudet (som ikke direkte befatter seg med behandlingsaktivitetene).»

Som nevnt har Datatilsynet pekt på at Telenor ASA mangler helt grunnleggende retningslinjer. Å kreve at rutinene hverken er motstridende eller feilaktige, er neppe å kreve særlig mye. Allerede her mener vi at Datatilsynets krav er innenfor det man med rimelighet kan forvente av Telenor ASA.

Videre har tilsynet avdekket noen policyer som ikke sier noe håndfast, og personvernarbeidet har funnet sted i kontekst av flere ulike fora. Ut fra den kompleksiteten som er avdekket gjennom tilsynet av Telenor ASAs organisering av personvernarbeidet og uklarheter rundt omfanget av behandlingsaktiviteter, vil det være forholdsmessig å utarbeide konkrete retningslinjer.

Vi mener at retningslinjer som handlet om personvernombudet hos Telenor ASA var mangelfulle. Dels gjenga de bare lovens ordlyd, dels var de selvmotsigende, og dels ga de ikke tilstrekkelig detaljerte anvisninger for personvernombudsordningen i Telenor ASA. Funnene og problemstillingene i dette vedtaket er i stor grad følgefeil av de mangelfulle retningslinjene. Det forelå ikke egnede organisatoriske tiltak for å sikre at rollen var faktisk

uavhengig, ble involvert i alle spørsmål som gjelder personvern og hadde tilgang til øverste ledelsesnivå i tråd med lovens intensjon.

For det femte mener vi at Telenor ASA mangler organisatoriske tiltak for å sikre generell overholdelse av personvernforordningen.

██████ skrev følgende i en e-post til ██████ datert 12. April 2021:

«Regarding Data Protection/Transfer Impact Assessments, the current backlog is quite big and I believe the organization is struggling a bit to get up to speed. There is currently little capacity/competency to conduct proper impact assessments among the ASA colleagues».²²⁰

Det eksterne personvernombudet ble satt på kopi i ovennevnte e-post og svarte blant annet:

«True. However, the lack of capacity/competence to conduct assessments is also a symptom of a more general issue of immature privacy compliance governance and performance at ASA, and a lack of foundational building blocks for privacy compliance, such as e.g. inventory, awareness and competence, operational capacity, implemented processes and unclear roles/responsibilities for group initiatives».²²¹

I forbindelse med en diskusjon om utkontraktering av operative oppgaver som gjaldt overholdelse av krav til personvern, skrev det eksterne personvernombudet følgende:

«However, more generally than simply discussing outsourcing of some operational privacy compliance activities (which also would have a time- (in terms of follow-up/involvement) and monetary cost to ASA), this discussion/issue between the mentioned entities foundationally has to do with defining each entity's role (privacy wise) and corresponding accountability, responsibilities and operational capacity in initiatives with group dependencies».²²²

Telenor ASA har informert oss om at det ikke ble noe av den aktuelle utkontrakteringen og at dette derfor er irrelevant.²²³ Etter vår oppfatning er den ovennevnte korrespondansen relevant, uavhengig av om utkontrakteringen fant sted eller ikke, fordi den illustrerer at det på det tidspunktet hersket usikkerhet i Telenor ASA om tildelingen av personvernroller (dvs. når Telenor ASA opptrer som behandlingsansvarlig, felles behandlingsansvarlig eller databehandler med eller for andre forretningsenheter), ansvarlighet og operativ kapasitet.²²⁴ Vi mener gjennomføringen av egnede organisatoriske tiltak i forbindelse med disse spørsmålene har vært mangelfull med tanke på å sikre og påvise at behandlingen utføres i samsvar med personvernforordningen.

²²⁰ «2021.04.13 – Mail to EVP People».

²²¹ «2021.04.13 – Mail to EVP People».

²²² «2021.04.13 – Mail to EVP People».

²²³ Endelig tilsynsrapport av 30. september 2022, s. 30.

²²⁴ Endelig tilsynsrapport av 30. september 2022, s. 30.

Ifølge det eksterne personvernombudet var det en generell pulverisering av ansvar²²⁵ og mangel på kompetanse i Telenor ASA.²²⁶ Basert på dokumentasjonen vi innhentet under dette tilsynet, er dette også vår vurdering. Vi viser til punkt 5.2.3 om vår vurdering av uklar ansvarsfordeling og rollefordeling i Telenor ASA.

Videre mener vi at de interne retningslinjene burde ha vært bedre strukturert på flere spesifikke og generelle personvernspørsmål, som det eksterne personvernombudet også påpekte.²²⁷ På møtet i GU Forum i september 2021 presenterte det eksterne personvernombudet blant annet følgende vedrørende personvern i Telenor ASA:

- «b) Routines, policies and documentation - The organization lacks structured and documented frameworks and ways-of-work to adhere to privacy requirements, causing inefficiencies, unclarity and direct non-compliance.
- c) Internal data sharing governance - Personal data is shared between business units within Telenor without adequate data sharing governance, including legal transfer mechanisms, clear definition of controller/processor relationships, and generally diffusion of responsibility.
- d) Business-, system- & contract ownership - Ambiguous/nonstandardized governance for internal business-, system- and contract ownership, as well as potential GSSoutsourcing/operation capacity, causing ambiguity and diffusion of responsibility for privacy compliance.
- e) Line org. capacity and competence - The organization lacks capacity and competence to deal adequately with privacy compliance pro-actively, causing strain on existing resource(s), process and progress bottlenecks, and ultimately low /noncompliance».²²⁸

I tillegg bemerket det eksterne personvernombudet risikoer med hensyn til personvernprinsippene, personvernerklæringer, brudd på personopplysningssikkerheten, vurderinger av personvernkonsekvenser (DPIA), deling av personopplysninger med tredjeparter som ikke overholder kravene («non-compliant»), og deling av personopplysninger med tredjeparter uten formelle lovbestemte krav, herunder internasjonale overføringer.²²⁹ Når denne typen alvorlige personvernrisikoer identifiseres, er det helt klart under personvernforordningen artikkel 24 nr. 1 at den behandlingsansvarlige må ta tak i dem. Det har Telenor ASA ikke gjort.

Vi merker oss at Telenor ASA har vedtatt interne prinsipper og retningslinjer for personvern²³⁰ som de hevder gjennomgås og oppdateres ved behov. En ny konsernhåndbok i

²²⁵ Se også punkt 5.2.3.

²²⁶ «2021.04.13 – Mail to EVP People».

²²⁷ «2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf»

²²⁸ «2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf», s. 13.

²²⁹ «2021.09.09 – TNASA Privacy status and proposals for GU Forum.pdf», s. 15-20.

²³⁰ «Group Policy Privacy, valid from: 2022-01-01»

«Group Manual Privacy, valid from: 2022-01-01»

«Group Manual Privacy, valid from: 01.06.2020»

«2020 Mandate and Functional Description Group Privacy and IM (share)»

personvern ble delt med oss 13. desember 2021, med gyldighet fra 1. januar 2022, som omfattet endringer i retning av bedre overholdelse av personvernforordningen. Dette er imidlertid ikke tilstrekkelig, ettersom det i tilsynsperioden manglet organisatoriske tiltak for å dekke problemstillinger nevnt ovenfor.

Hvis det i denne saken var snakk om en liten virksomhet med få ansatte kunne det tenkes at mer uformelle rutiner var tilstrekkelig, men dette er lite praktisk i en virksomhet med stort forretningsområde og mange ansatte. I denne sammenhengen viser vi til at Telenor ASA er et morselskap i et av de største norske konsernene i telekomsektoren. På tilsynstidspunktet hadde Telenor ASA ansvar for å sette globale policies, og vi mener det må kunne forventes at morselskapet som setter policy på personvernområdet selv klarer å operasjonalisere disse gjennom konkrete rutiner og retningslinjer. Manglende konkrete retningslinjer står også i kontrast til Telenor ASAs virksomhet ellers som er styrt av mange konserninterne styringsdokumenter. Som Telenor ASA også viser til i tilsvaret så opererer de i en sektor som er strengt lovregulert med stor vekt på etterlevelse (compliance). Det er da naturlig å stille tilsvarende krav til etterlevelse på personvernområdet som for andre forretningskritiske områder.

Det eksterne personvernombudet beskrev at det forelå risiko for at rollen ikke kunne utføres på en uavhengig og god måte.²³¹ Etter vår mening var en av årsakene til dette manglende iverksetting av klare retningslinjer, herunder avklart rapporteringslinje og tilgang til øverste ledelse og tydelig angivelse av personvernombudets oppgaver.

Samlet sett er vår vurdering at Telenor har brutt personvernforordningen artikkel 24 nr. 1 og 2 ved å ikke å ha innført egnede organisatoriske tiltak for å sikre og påvise etterlevelse og ved å ha hatt mangelfulle retningslinjer.

13 Vurdering av korrigerende tiltak

13.1 Oppsummering av konklusjoner med hensyn til korrigerende tiltak

Med henvisning til vurderingene i punkt 5 bemerker vi at Telenor ASA ikke har gjort en intern og dokumentert analyse av forpliktelsen om å utpeke et personvernombud, som er en nødvendig del av internkontrollen og dermed er i strid med personvernforordningen artikkel 24.

Videre i punkt 5 pekte vi på at Telenor ASA selv har innrømmet at selskapet ikke har hatt tilstrekkelige rutiner hva gjelder utfylling og oppdatering av behandlingsprotokollen. Telenor ASA mener selv at protokollen inneholder uklarheter.²³² Som påpekt i punkt 5 er protokollen en del av internkontrollen, og personvernforordningen artikkel 24 krever organisatoriske tiltak for å sørge for at behandlingsprotokollen til enhver tid er korrekt og oppdatert.

«Old Group Privacy IM mandate (pre 2021)», 1. mars 2020.

²³¹ «2021.09.09 – TNASA Privacy status and proposals for GU Forum», s. 13.

²³² Merknader til forhåndsvarsel av 31. mai 2024, s. 11.

Med henvisning til vurderingene i punkt 8 kom vi til at Telenor ASA ikke hadde etablert en formell, direkte rapporteringslinje for personvernombudet til den øverste ledelsen under størsteparten av tilsynsperioden, i strid med personvernforordningen artikkel 38 nr. 3.

Med henvisning til vurderingene i punkt 12 kom vi til at Telenor ASA ikke har gjennomført organisatoriske tiltak for å sikre og påvise etterlevelse av personvernforordningen, i strid med personvernforordningen artikkel 24 nr. 1, og ikke har innført egnede retningslinjer, i strid med personvernforordningen artikkel 24 nr. 2, hva gjelder organisatoriske tiltak knyttet til personvernforordningen artikkel 38 og generell etterlevelse av personvernforordningen.

Når det gjelder delvis overtredelse av personvernforordningen artikkel 37 nr. 7, merker vi oss dette som en mindre overtredelse for en begrenset periode, som har blitt korrigert. Vi vurderer derfor at det ikke trengs ytterligere handling eller korrigerende tiltak.

Datatilsynet konkluderte under tvil at Telenor ASA ikke har gitt personvernombudet tilstrekkelige ressurser etter personvernforordningen artikkel 38 nr. 2, men siden Telenor ASA for tiden ikke har personvernombud, ilegger vi heller ikke korrigerende tiltak for dette.

13.2 Pålegg om tiltak

Basert på funnene i punkt 13.1 har vi kommet frem til at det er nødvendig å reagere på disse overtredelsene. Vi pålegger Telenor ASA følgende tiltak, jf. personvernforordningen artikkel 24 nr. 1 og 2:

- Å lage en dokumentert intern analyse om hvorvidt Telenor ASA er forpliktet å utpeke personvernombud som tar bl.a. hensyn til Telenor ASAs rolle i de forskjellige behandlingsaktiviteter.

Vi viser til punkt 5.2.1 hvor vi omtaler at Telenor ASA ikke har lagt frem dokumentert vurdering av spørsmålet om Telenor ASA er forpliktet til å utpeke personvernombud i sine roller som behandlingsansvarlig, felles behandlingsansvarlig og databehandler. Slik vurdering skal gjennomføres som et organisatorisk tiltak og dokumenteres som en del av internkontrollen²³³ jf. personvernforordningen artikkel 24, hvis det ikke er åpenbart unødvendig.²³⁴ Tatt i betraktning uklarheter rundt Telenor ASAs rolle, samt at virksomhetens behandlingsprotokoll oppgir langt flere behandlingsaktiviteter med større omfang enn rene HR-oppgaver i Telenor ASA og høyt antall registrerte i flere land, mener vi denne vurderingen er nødvendig.

- Å revidere behandlingsprotokollen etter personvernforordningen artikkel 30 og iverksette organisatoriske tiltak for å sikre at den til enhver tid gir en oppdatert beskrivelse av behandlingsaktivitetene i Telenor ASA, antall registrerte og rollene Telenor ASA har.

²³³ Jarbekk m.fl. Eva Jarbekk mfl.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019), s. 256.

²³⁴ WP 243 rev.01 «Retningslinjer for databeskyttelsesrådgivere», s. 5-6.

Vi viser til punkter 5.2.2 og 5.2.3 hvor vi omtaler Telenor ASAs behandlingsprotokoll. Det å føre og vedlikeholde slik protokoll, jf. personvernforordningen artikkel 30, faller også under obligatorisk internkontroll og organisatoriske tiltak som Telenor ASA må gjennomføre etter personvernforordningen artikkel 24.²³⁵ Behandlingsprotokollen er viktig dokument som skal gi reell oversikt over selskapets behandlingsaktiviteter og roller.

- I tilfelle Telenor ASA faktisk er forpliktet til å ha et personvernombud, å gjennomføre organisatoriske tiltak og innføre egnede retningslinjer med hensyn til personvernombudets organisering. Dette inkluderer beskrivelse av rapporteringslinje til tydelig definert øverste ledelsesnivå, beskrivelse av hvilke oppgaver personvernombudet bør involveres i, samt på hvilken måte og hva som er rett tid. Vurderinger og tiltak for å sikre uavhengighet og at det ikke foreligger interessekonflikter inkluderer å skille klart mellom eventuelle andre roller i stillingsbeskrivelse, sørge for egen e-postadresse for personvernombudet og gjøre en dokumentert vurdering av ombudets aksjeeierskap i selskapet.

Vi viser til punkt 12.

Vårt rettslige grunnlag for å utstede dette pålegget er personvernforordningen artikkel 58 nr. 2 bokstav d.

Som nevnt er det en forutsetning for at behandlingsaktiviteter er i samsvar med forordningen at behandlingsansvarlig oppfyller alle sine plikter i henhold til personvernforordningen kapittel IV. Vi mener derfor at tilsynets myndighet etter artikkel 58 nr. 2 bokstav d ikke er begrenset til behandlingsaktiviteter som sådan, men alle forholdene som kreves for etterlevelse av personvernforordningen.²³⁶ Dette støttes også av artikkel 57 nr. 1 bokstav a, som slår fast det er tilsynsmyndighetens oppgave å føre tilsyn med og håndheve anvendelsen av personvernforordningen. EU-domstolen har uttalt at bruk av korrigerende tiltak skal «sikre et ensartet og højt niveau for beskyttelse af personoplysninger gennem en effektiv håndhævelse» og at formålet med personvernforordningen artikkel 58 nr. 2 er «at sikre, at behandlingen af personoplysninger sker i overensstemmelse med denne forordning, og at tilfælde af brud på sidstnævnte forordning genoprettes for at bringe disse i overensstemmelse med EU-retten ved de nationale tilsynsmyndigheders indgriben (...)».²³⁷

Det er i alle tilfeller klart at Datatilsynet kan ilegge overtredelsesgebyr for en rekke lovbrudd som ikke direkte gjelder en konkret behandlingsaktivitet som sådant. I noen tilfeller er det mer hensiktsmessig og forholdsmessig å ilegge mildere forvaltningsreaksjoner som pålegg enn å

²³⁵ Åste Marie Bergseng Skullerud, Cecilie Rønnevik, Jørgen Skorstad og Marius Engh Pellerud: *Personopplysningsloven og personvernforordningen, kommentarutgave* (2019) s. 273 og 276, Eva Jarbekk mfl.: *Personopplysningsloven og personvernforordningen med kommentarer* (2019) s. 257.

²³⁶ Telenor ASA hevder på side 51 i tilsvaret av 31. mai 2024 at vi ikke kan ilegge pålegg fordi påleggene ikke angår utførelsen av behandlingsaktivitetene..

²³⁷ EU-domstolens dom i sak C-768/21 *Land Hessen*, avsnitt 38 og 45.

ilegge overtredelsesgebyr. Tilsvarende gjelder for irrettesettelse, som fortalepunkt 148 eksplisitt slår fast kan ilegges i stedet for overtredelsesgebyr.

Vurdering av om utpeking av personvernombud er en forpliktelse, og uriktigheter i behandlingsprotokollen har i utgangspunktet ikke vært et spesifikt tema under tilsynet, men ble tatt opp av Telenor ASA i merknader til forhåndsvarsel. Vi mener det ikke er nødvendig og forholdsmessig i forhold til disse overtredelsene å ilegge overtredelsesgebyr.

Fristen for å oppfylle påleggene vil være **3 måneder** fra tidspunktet Telenor ASA mottok vedtaket, og hvor Telenor ASA bes om å sende oss en dokumentert bekreftelse på at pålegget er oppfylt innen denne fristen.

13.3 Irrettesettelse

Irrettesettelse er en forvaltningsmessig reaksjon med formål å markere kritikk av de omtalte bruddene på reglene. Ileggelse av irrettesettelse vil kunne bli lagt vekt på i en eventuell senere vurdering av ileggelse av overtredelsesgebyr hvis det forekommer tilsvarende brudd på regelverket, jf. personvernforordningen art. 83 nr. 2 bokstav i.

Personvernombud spiller en viktig rolle i å bistå den behandlingsansvarlige/databehandler med å sikre overholdelse av kravene i personvernforordningen og sørge for at de registrertes grunnleggende rettigheter blir ivaretatt. Forpliktelsene i personvernforordningen artikkel 38 er grunnleggende krav som må oppfylles for å ha et funksjonelt personvernombud. Kravene er like uansett om personvernombudet er obligatorisk eller frivillig. Vi legger til grunn at overtredelse av disse bestemmelsene fører til at personvernombudet blir ineffektivt, noe som igjen kan påvirke de registrertes rettigheter og at behandlingsaktiviteter ikke skjer i tråd med loven. Dette tilsier i utgangspunktet at tilsynet kan reagere med overtredelsesgebyr. I noen saker foreligger det likevel forhold som tilsier at irrettesettelse er passende reaksjon.

Som en konsekvens av varsel om vedtak valgte Telenor ASA å avslutte ordningen med personvernombud. Dette er etter vårt syn svært beklagelig. Etter vår vurdering krever dette en grundigere vurdering enn det som er foretatt da det ikke er åpenbart at Telenor ASA ikke faller innunder kravet om å ha personvernombud. Hvis Telenor ASA etter en slik vurdering fastholder at personvernombudsrollen deres er frivillig, så vil vi likevel oppmuntre til at selskapet gjeninnfører ombudet. Særlig bør det tas i betraktning at det fremkom under tilsynet og senere at personvernombudet i praksis har dedikert hundre prosent av sin tid til rollen, samtidig som det har vært personvernombudsoppgaver vedkommende ikke har hatt mulighet til å utføre. Slik selskapet selv har beskrevet behovet for personvernarbeid er det derfor et paradoks at de velger å avslutte ombudsrollen i stedet for å sørge for at den både utføres i tråd med forordningen og med tilstrekkelige ressurser.

Vi er imidlertid enig med Telenor ASA at det kan gi en uheldig signaleffekt ut over denne saken dersom det ilegges overtredelsesgebyr for noe som er en frivillig ordning, og derfor bør terskelen for dette ligge høyt. Hensynet bak personvernombudsrollen er nettopp å bidra til virksomhetenes etterlevelse og personvernkultur, og Datatilsynet ser helst at flere

virksomheter har ombud. Vi vil likevel understreke at de forhold som ble avdekket under tilsynet og som vi har vurdert etter ytterligere informasjon fra Telenor ASA, tilsier at det foreligger brudd på personvernforordningen artikkel 38 nr. 3 som gir grunnlag for overtredelsesgebyr. Saken kunne derfor stilt seg annerledes dersom Telenor ASA åpenbart falt innenfor plikten etter personvernforordningen artikkel 37 til å oppnevne personvernombud.

Vi anser det som nødvendig å reagere på overtredelsene, og tatt i betraktning det ovennevnte, ilegger vi en irettesettelse for brudd på personvernforordningen artikkel 38. nr. 3 siste punktum for

- *å ikke ha på plass rapporteringslinje for personvernombudet i Telenor ASA til øverste ledelsesnivå for ca. ett år av tilsynsperioden.*

Vårt rettslige grunnlag for å utstede denne irettesettelsen er personvernforordningen artikkel 58 nr. 2 bokstav b.

13.4 Vurdering av om det skal ilegges overtredelsesgebyr

I det videre vil vi vurdere ileggelse av overtredelsesgebyr for bruddene på personvernforordningen artikkel 24 nr. 1 og 2 når det gjelder mangelfulle organisatoriske tiltak knyttet til personvernforordningen artikkel 38 og generell etterlevelse av personvernforordningen.

13.4.1 Generelle prinsipper ved vurdering av overtredelsesgebyr

En «administrativ sanksjon» er 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 menneskerettighetskonvensjon (EMK).²³⁸

Høyesterett (Rt. 2012 s. 1556) har konkludert med at et overtredelsesgebyr er å anse som straff etter EMK artikkel 6. Vi kan derfor bare ilegge et gebyr der det foreligger klar sannsynlighetsovervekt for brudd på personvernforordningen. I denne saken er det klar sannsynlighetsovervekt for alle bruddene som overtredelsesgebyret ilegges for. For å ilegge en administrativ sanksjon, for eksempel et overtredelsesgebyr, må legalitetsprinsippet være oppfylt. Legalitetsprinsippet er et generelt prinsipp i både EØS-retten²³⁹ og norsk forvaltningsrett.²⁴⁰

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

²³⁸ Forvaltningsloven § 43.

²³⁹ EFTA-domstolen, sak E-9/11 side 29 avsnitt 99.

²⁴⁰ Grunnloven § 113.

I fortalepunkt 148 er dette utdypet:

«For å styrke håndhevingen av bestemmelsene i denne forordning bør det ved overtredelse av denne forordning ilegges sanksjoner, herunder overtredelsesgebyr, i tillegg til eller i stedet for egnede tiltak som tilsynsmyndigheten pålegger i henhold til denne forordning.»

Vilkårene for ileggelse av gebyr fremgår av forordningen artikkel 83. Bestemmelsen gir i utgangspunktet anvisning på at ileggelse av overtredelsesgebyr beror på en skjønnsmessig helhetsvurdering, men legger føringer på skjønnsutøvelsen ved å trekke frem momenter som skal tillegges særlig vekt, jf. personvernforordningen artikkel 83 nr. 2 bokstav a til k.

EU-domstolen presiserte i sin avgjørelse av 5. desember 2023 i sak C-807/21 (*Deutsche Wohnen*) at vilkårene for ileggelse av overtredelsesgebyr er uttømmende regulert i personvernforordningen artikkel 83 nr. 1 til 6. Domstolen kom til at artikkel 83 skal forstås slik at ileggelse av overtredelsesgebyr er betinget av at den behandlingsansvarlige har utvist skyld i form av uaktsomhet eller forsett. 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.

Når det gjelder formålet med bestemmelsene i personvernforordningen, har EU-domstolen uttalt at det er:

«... at sikre et ensartet og høyt nivå for beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger i EU og med henblik herpå at sikre en konsekvent og ensartet anvendelse af reglerne for beskyttelse af disse personers grundlæggende rettigheder og frihedsrettigheder i forbindelse med behandling af sådanne oplysninger overalt i EU.»²⁴¹

«De administrative bøder bidrager på grund af deres afskrækkende virkning til at styrke beskyttelsen af fysiske personer i forbindelse med behandling af personoplysninger og udgør derfor et centralt element til at sikre overholdelsen af disse personers rettigheder i overensstemmelse med forordningens formål om at sikre et højt beskyttelsesniveau for sådanne personer i forbindelse med behandling af personoplysninger.»²⁴²

13.4.2 Lovkrav

Avhengig av omstendighetene i hvert enkelt tilfelle skal overtredelsesgebyr ilegges jf. personvernforordningen artikkel 58 nr. 2 bokstav i), i tillegg til eller i stedet for øvrige

²⁴¹ EU-domstolen sak C-807/21 *Deutsche Wohnen mot Staatsanwaltschaft Berlin*, avsnitt 72

²⁴² EU-domstolen sak C-807/21 *Deutsche Wohnen mot Staatsanwaltschaft Berlin*, avsnitt 73

sanksjoner nevnt i personvernforordningen artikkel 58 nr. 2 bokstav a) - h) og j), jf. artikkel 83 nr. 2 første punktum.

Personvernforordningen artikkel 24 er ikke nevnt i oppregningen i forordningen artikkel 83 nr. 4 og 5. Brudd på denne bestemmelsen kan derfor bare sanksjoneres med overtredelsesgebyr dersom det er bestemt i nasjonal rett. For personvernforordningen artikkel 24 er det gitt en slik hjemmel i personopplysningsloven § 26 første ledd, jf. personvernforordningen artikkel 84.

13.4.3 Momenter som skal tillegges særskilt vekt ved vurdering av gebyr

I vurderingen av om overtredelsesgebyr skal ilegges, skal Datatilsynet legge vekt på momentene i personvernforordningen artikkel 83 nr. 2 bokstav a til k. Under følger vår vurdering av de momentene vi anser som relevante i vurderingen av om overtredelsesgebyr skal ilegges for brudd på personvernforordningen artikkel 24 nr. 1 og nr. 2.

a) *Overtredelsens karakter, alvorlighetsgrad og varighet*

Når det gjelder kriteriet i personvernforordningen artikkel 83 nr. 2 bokstav a, kan Telenor ASAs overtredelser, som beskrevet ovenfor, ilegges straffesanksjon i henhold til det laveste av de to nivåene fastsatt i personvernforordningen jf. personvernforordningen artikkel 83 nr. 4.

Når det gjelder overtredelsenes *karakter*, er plikten til å gjennomføre egnede organisatoriske tiltak og innføre egnede retningslinjer etter personvernforordningen artikkel 24 nr. 1 og 2 utslag av det grunnleggende ansvarlighetsprinsippet. Ansvarlighetsprinsippet ligger til grunn for alle virksomhetens plikter og er en forutsetning for reell, systematisk og effektiv etterlevelse av personvernforordningen. Bruddet angår altså en sentral og grunnleggende norm i personvernforordningen, noe som er skjerpene.

Når vi vurderer overtredelsens *alvorlighetsgrad*, tar vi hensyn til *behandlingens art*, dvs. forretningsaktivitet. Vi legger mer vekt på overtredelsens alvorlighetsgrad når det er en klar ubalanse mellom de registrerte og den behandlingsansvarlige, slik som i dette tilfellet, der de fleste av de registrerte er ansatte.²⁴³

Når det gjelder *omfanget av behandlingen*, er det som nevnt uklart hvilke behandlinger Telenor ASA er behandlingsansvarlig for, hvilket igjen påvirker omfanget av ansvaret under personvernforordningen artikkel 24.

Denne uklarheten gjør det også vanskelig å slå fast hva *formålet med behandlingen* er. Ifølge Telenor ASA er formålet hovedsakelig HR-administrasjon og behandling av ansattes personopplysninger.

Det er også vanskelig å anslå *antallet registrerte som er berørt*. Telenor ASA har om lag 380 ansatte, men det er usikkert nøyaktig hvor mange som er berørt. Telenor ASAs artikkel 30-

²⁴³ Retningslinjer 04/2022 om beregning af administrative bøder i henhold til databeskyttelsesforordningen, s. 20.

protokoll viser at antall registrerte som omfattes av behandlingsaktiviteter som Telenor ASA utførte i tilsynsperioden, varierte fra maksimalt 25 000–100 000 registrerte til minimum 1–25 registrerte.²⁴⁴ I tillegg er alle ansatte i konsernet, ca. 15 000 registrerte, berørt av behandling som utføres av datterselskaper, som Telenor ASA ifølge behandlingsprotokollen har et felles behandlingsansvar for, jf. punkt 5.2.3.

Videre er et høyt antall kunder nevnt som registrerte i behandlingsprotokollen i forbindelse med felles behandlingsansvar med Telenors datterselskaper. Telenor ASA opplyser i tilsvaret at oppføringen i protokollen ikke stemmer med realiteten. Datatilsynet bemerker viktigheten av at behandlingsprotokollen er gir et korrekt bilde av behandlingsaktiviteter i virksomheten. Både for at selskapet må ha en oversikt selv og fordi det er sentral dokumentasjon for tilsynets vurderinger.

På grunn av uklarhetene i dokumentasjonen Telenor ASA har forelagt Datatilsynet, kan vi ikke slå fast hvor mange registrerte som er berørt av overtredelsen.

Det er ikke nødvendig å identifisere noen spesifikke skader for å fastslå at et brudd har funnet sted, men *omfanget av skade* skal tas med som et moment i vurderingen. Vi anser det som en formildende faktor at det ikke er avdekket noen spesifikk skade på de registrertes personvern, samtidig som vi minner om at det kan være vanskelig for de registrerte å finne ut om personopplysningene deres har blitt behandlet i strid med personvernforordningen.

Vurderingen av overtredelsens *varighet* er begrenset til tilsynsperioden, som er perioden fra 10. oktober 2020 til 28. januar 2022. Vi vil bare vurdere varigheten av overtredelsene i denne perioden. Situasjonen før eller etter denne perioden tas ikke med i vurderingen som skjerpene eller formildende faktorer i denne sammenhengen.

Overtredelsen av personvernforordningen artikkel 24 nr. 1 og 2 om organisatoriske tiltak og iverksetting av egnede retningslinjer foregikk i hele tilsynsperioden. Vi viser til punkt 12.2.

Vi mener at overtredelsens varighet på ca 15 måneder i dette tilfellet utgjør en skjerpene faktor.

Til tross for at det ikke kan påvises håndfast skade på de registrertes personvern samt uklarheter rundt behandlingens omfang, formål og antall registrerte, mener vi at karakteren og varigheten av overtredelsen tilsier illeggelse av overtredelsesgebyr.

b) hvorvidt overtredelsen ble begått forsettlig eller uaktsomt

Illeggelse av overtredelsesgebyr er betinget av at den behandlingsansvarlige har utvist skyld i form av uaktsomhet eller forsett, jf. personvernforordningen artikkel 83 nr. 2 bokstav b, sammenholdt med artikkel 83 nr. 3, jf. EU-domstolens avgjørelser datert 5. desember 2023 i sakene C-807/21 (Deutsche Wohnen) og C-683/21. I førstnevnte avgjørelse uttaler EU-domstolen:

²⁴⁴ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

«Det følger således af ordlyden af databeskyttelsesforordningens artikel 83, stk. 2, at det kun er overtrædelser af denne forordnings bestemmelser, der er begået culpøst af den dataansvarlige, dvs. overtrædelser begået forsætligt eller uagtsomt, der kan føre til, at denne pålægges en administrativ bøde i henhold til denne artikel.»²⁴⁵

Se også forvaltningsloven § 46 første ledd.

Uaktsomhet er definert slik i straffeloven § 23:

«Den som handler i strid med kravet til forsvarlig opptreden på et område, og som ut fra sine personlige forutsetninger kan bebreides, er uaktsom. Uaktsomheten er grov dersom handlingen er svært klanderverdig og det er grunnlag for sterk bebreidelse.»

I henhold til kravet om forsvarlig opptreden må foretak og ansvarlige personer som opptrer på deres vegne, undersøke rettskravene som gjelder for deres felt og gjennomføre disse. Ellers kan selskapet anses å ha handlet uaktsomt når det gjelder denne feilen.

Høyesterett har slått fast at det ikke er nødvendig å påvise at en identifisert enkeltperson har opptrådt uaktsomt eller forsettlig på vegne av selskapet, og at anonyme eller kumulative feil begått av enkeltpersoner som opptrer på vegne av selskapet, kan anses å oppfylle skyldkravet, så lenge minstekravet til uaktsomhet er oppfylt.²⁴⁶

Telenor Group er et ledende teleselskap i Norden og Asia med 209 millioner abonnenter og en årlig omsetning på rundt 81 milliarder kroner (2023),²⁴⁷ der Telenor ASA er morselskapet. Etter vårt syn har Telenor ASA midler og kompetanse til å sette seg godt inn i rettskravene som gjelder på personvernområdet og bør opptre deretter.

Etter vårt syn har ikke Telenor ASA satt seg tilstrekkelig inn hva som kreves etter personvernforordningen artikkel 24, noe de mangelfulle vurderingene, tiltakene og retningslinjene vitner om. Informasjonen under tilsynet viser at selskapet ikke prioriterte og satte av nok ressurser til å ta tak i problemene identifisert av det eksterne personvernombudet, herunder hva gjelder internkontroll, på tross av en klar oppfordring om å gjøre det. Med andre ord har selskapet ikke gjort det som kunne forventes, og det har ikke operert i henhold til kravet om forsvarlig opptreden. Derfor ble lovbruddet i alle fall begått uaktsomt. Følgelig finner vi at det foreligger en straffbar overtredelse, som er et vilkår for å ilegge overtredelsesgebyr.²⁴⁸

Vi anser skyldkravet oppfylt og at det taler for ileggelse av overtredelsesgebyr.

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

²⁴⁵ EU-domstolen sak C-807/21 *Deutsche Wohnen v Staatsanwaltschaft Berlin*, avsnitt 68

²⁴⁶ Jf. HR-2022-1271-A avsnitt 36–50.

²⁴⁷ <https://www.telenor.com/about/>, sist besøkt 11. april 2024.

²⁴⁸ EU-domstolen sak C-807/21 *Deutsche Wohnen mot Staatsanwaltschaft Berlin*, avsnitt 75

Det er ikke påvist noen materiell skade som de registrerte har lidd. Dette kriteriet kommer derfor ikke til anvendelse i denne saken.

d) den behandlingsansvarliges eller databehandlerens grad av ansvar, idet det tas hensyn til de tekniske og organisatoriske tiltak de har gjennomført i henhold til artikkel 25 og 32

Vi er enige med Telenor ASA at dette kriteriet gjelder ikke i denne tilsynssaken, da tekniske og organisatoriske tiltak i henhold til personvernforordningen artikkel 25 og 32 ikke har vært et tema.

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

Dette kriteriet gjelder ikke i denne saken, da Telenor ASA ikke tidligere har vært ilagt sanksjoner for tilsvarende eller på annen måte «relevante» overtredelser.

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

Telenor ASA har vært samarbeidsvillige gjennom hele tilsynet, ved å gi informasjon og svare på våre spørsmål. Vi vurderer at denne faktoren verken er en skjerpene eller en formildende faktor.²⁴⁹

g) kategoriene av personopplysninger som er berørt av overtredelsen

Kategorier av personopplysninger knyttet til Telenor ASAs egne ansatte omfatter kontaktopplysninger, opplysninger om karriere og kompetanse, kommunikasjon, lokalisering, atferd, regnskap og balanse, finansielle transaksjoner og familieforhold.²⁵⁰ Noen av disse kategoriene av personopplysninger kan anses som sensitive for den registrerte (som opplysninger om økonomi), selv om de ikke faller inn under personvernforordningen artikkel 9 nr. 1.

Bare en begrenset mengde av kategoriene faller inn under definisjonen av særlige kategorier av personopplysninger i henhold til artikkel 9 nr. 1, herunder helseopplysninger om ansatte og politiattest for arbeidssøkere.²⁵¹

Kategorier av personopplysninger knyttet til kunder omfatter atferd, preferanser, interesser, demografi, identitet, lokalisering og fysiske egenskaper (ikke helsesrelaterte).²⁵² Telenor ASA

²⁴⁹ Ifølge WP253 Retningslinjer vedrørende anvendelse og fastsettelse af administrative bøder i overensstemmelse med forordning (EU) 2016/679, s. 15 kan bokstav f være en formildende faktor i noen tilfeller, men det vil ikke være hensiktsmessig å ta hensyn til samarbeid som allerede er lovpålagt.

²⁵⁰ Endelig tilsynsrapport av 30. september 2022, s. 5.

²⁵¹ Endelig tilsynsrapport av 30. september 2022, s. 5.

²⁵² Endelig tilsynsrapport av 30. september 2022, s. 5.

behandler også enkelte kategorier av personopplysninger knyttet til andre personer, herunder for eksempel konsulenter og leverandører.²⁵³

Det er vanskelig å slå fast nøyaktig hvilke kategorier av personopplysninger som er berørt av overtredelsen, på grunn av uklarhetene i dokumentasjonen Telenor ASA har forelagt Datatilsynet.

Vi mener at dette kriteriet i sum utgjør verken en skjerpende eller formildende faktor.

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 ble kjent med overtredelsen gjennom igangsetting av tilsynet. I denne saken anser vi dette som verken en skjerpende eller formildende faktor.

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

Dette er verken en formildende eller en skjerpende faktor, da vi ikke har pålagt noen tidligere korrigerende tiltak mot Telenor ASA med hensyn til samme saksgjenstand.

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

Dette kriteriet kommer ikke til anvendelse i denne saken.

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

Datatilsynet har ingen opplysninger som tyder på at Telenor ASA har hatt økonomiske fordeler av overtredelsene.

Som forklart over var det vanskelig å konkludere i vurderingen av flere av momentene ovenfor fordi omfanget av Telenor ASAs behandlingsansvar er uklart. Dette er en konsekvens av at Telenor ASA ikke har hatt tilstrekkelige organisatoriske tiltak for å føre og vedlikeholde behandlingsprotokoll, jf. punkt 5 og 13.2. Datatilsynet anser dette som en skjerpende faktor.

Som beskrevet i de foregående avsnittene, har Telenor ASA truffet noen tiltak i løpet av 2021 og etablert rapporteringslinje for personvernombudet til GU Forum og la til en eskaleringsmulighet til CEO og styret. Dette anser vi som formildende faktorer.

²⁵³ Telenor ASAs artikkel 30-protokoll av 2. februar 2022.

13.4.4 Konklusjon om hvorvidt det skal ilegges overtredelsesgebyr

Telenor ASA er morselskapet til et stort konsern i en strengt regulert telekombransje og burde være rustet til å ha god internkontroll. Tatt i betraktning momentene i personvernforordningen artikkel 83 nr. 2, tilsier omstendighetene i saken at det skal ilegges et overtredelsesgebyr.

Datatilsynet mener at ilegging av overtredelsesgebyr er berettiget med henblikk på å gi en reell avskrekkende effekt og motvirke at Telenor ASA – samt selskaper i Telenor Group og andre selskaper generelt – begår lignende overtredelser i fremtiden, og at de sørger for god internkontroll, herunder å gjennomføre nødvendige tiltak og vurderinger samt dokumentasjon av disse. Sanksjoner bør skape tilstrekkelig press til at manglende oppfyllelse i praksis er økonomisk uattraktivt.²⁵⁴

13.5 Fastsettelse av overtredelsesgebyr

Etter å ha tatt behørig hensyn til de forhold som er nevnt i personvernforordningen artikkel 83 nr. 1 og 2, finner vi at et overtredelsesgebyr på **4 000 000 NOK** er passende i denne saken. Årsakene til dette er beskrevet under.

I den forbindelse bør det bemerkes at fastsettelse av et gebyr ikke er en aritmetisk nøyaktig utøvelse,²⁵⁵ og at tilsynsmyndighetene kan utøve et visst skjønn i så henseende.²⁵⁶ De bør likevel angi faktorene som påvirket skjønnsutøvelsen i forbindelse med fastsettelse av gebyret.²⁵⁷

Personvernforordningen artikkel 83 nr. 1 fastsetter følgende når det gjelder overtredelsesgebyrets størrelse:

«Hver tilsynsmyndighet skal sikre at ilegging av overtredelsesgebyr i henhold til denne artikkel for overtredelser av denne forordning nevnt i nr. 4, 5 og 6 i hvert enkelt tilfelle er virkningsfull, står i et rimelig forhold til overtredelsen og virker avskrekkende.»

I henhold til personvernforordningen artikkel 83 nr. 2 skal det ved avgjørelsen av overtredelsesgebyrets størrelse i hvert enkelt tilfelle tas behørig hensyn til de forhold som er nevnt i artikkel 83 nr. 2 bokstav a–k.

Fortalepunkt 148 understreker det at det bør ilegges overtredelsesgebyrer «for å styrke håndhevingen av bestemmelsene i denne forordning».

²⁵⁴ Se generaladvokat Geelhoeds uttalelse i sak C-304/02, *Kommisjonen mot Frankrike*, avgitt 29. april 2004, avsnitt 39.

²⁵⁵ Se blant annet sak T-425/18, *Altice Europe NV mot Kommisjonen*, avsnitt 362; sak T-11/06, *Romana Tabacchi mot Kommisjonen*, avsnitt 266.

²⁵⁶ Se blant annet sak T-192/06, *Caffaro Srl mot Kommisjonen*, avsnitt 38.

²⁵⁷ EDPB Afgørelse 01/2022 om tvisten vedrørende den franske tilsynsmyndigheds udkast til afgørelse om Accor SA i henhold til artikkel 65, stk. 1, litra a), i GDPR, avsnitt 75.

Fortalepunkt 150 fastslår:

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

I henhold til EU-domstolens rettspraksis må begrepet «foretak» forstås som en økonomisk enhet, selv om denne økonomiske enheten består av flere juridiske personer.²⁵⁸ Ulike selskaper som tilhører samme konsern og utgjør en økonomisk enhet, regnes derfor som et «foretak» i henhold til artikkel 101 og 102 i TEUV (traktaten om Den europeiske unions virkemåte).

Telenor ASA er morselskap i Telenor Group. Telenor Group må regnes som en økonomisk enhet og dermed også SEU («Single Economic Unit»), dvs. som det relevante foretaket for utregning av overtredelsesgebyret.²⁵⁹ Personvernrådet har fattet en bindende beslutning med pålegg til tilsynsmyndigheten om å ta hensyn til den samlede omsetningen til alle enhetene som utgjør det enkelte foretaket, dvs. den konsoliderte omsetningen til konsernet med morselskapet i spissen.²⁶⁰ EU-domstolen har fastslått at maksimalbeløpet for overtredelsesgebyret utregnes på grunnlag av en prosentandel av foretakets samlede globale årsomsetning i forutgående regnskapsår.²⁶¹

Overtredelsene i denne saken kvalifiserer for overtredelsesgebyr i henhold til personvernforordningen artikkel 83 nr. 4 bokstav a. Maksimalbeløpet i henhold til artikkel 83 nr. 4 er 10 000 000 euro eller, dersom det dreier seg om et foretak, opptil 2 % av den samlede globale årsomsetningen i forutgående regnskapsår, *der det høyeste beløpet anvendes*.

Når det gjelder kravene etter personvernforordningen artikkel 83 nr. 1 for å sikre at ilegging av overtredelsesgebyret under omstendighetene i saken er virkningsfullt, står i et rimelig forhold til overtredelsen og virker avskrekkende, må det tas hensyn til Telenor Groups økonomiske stilling. Konsernets økonomiske stilling er også relevant for å fastsette det maksimale gebyret i denne saken.

Ved utregning av overtredelsesgebyret tar Datatilsynet hensyn til Telenor Groups årsomsetning.²⁶² Ifølge regnskapet i Telenor Groups årsrapport for 2023 var Telenor Groups

²⁵⁸ EU-domstolen sak C-516/15 P *Akzo Nobel m. fl mot Kommisjonen*, avsnitt 48, med videre henvisninger. EU-domstolen sak C-807/21 *Deutsche Wohnen mot Staatsanwaltschaft Berlin*, avsnitt 56.

²⁵⁹ EDPB Retningslinjer 04/2022 om beregning af administrative bøder i henhold til databeskyttelsesforordningen, s. 38.

²⁶⁰ EDPB Bindende afgørelse 1/2023 om den tvist, der er indbragt af den irske tilsynsmyndighed om Meta Platforms Ireland Limited's dataoverførsler for selskabets Facebooktjeneste (artikel 65 i GDPR), vedtatt 13. april 2023, avsnitt 365

²⁶¹ EU-domstolen sak C-807/21 *Deutsche Wohnen mot Staatsanwaltschaft Berlin*, avsnitt 57.

²⁶² EDPB Retningslinjer 04/2022 om beregning af administrative bøder i henhold til databeskyttelsesforordningen, s. 38; EDPB Bindende afgørelse 1/2023 om den tvist, der er indbragt af den irske tilsynsmyndighed om Meta Platforms Ireland Limited's dataoverførsler for selskabets Facebooktjeneste (artikel 65 i GDPR), vedtatt 13. april 2023, avsnitt 365

samlede omsetning i 2023 på 80 452 000 000 kroner,²⁶³ eller ca. 7 157 332 860 euro.²⁶⁴ I denne saken er det tillatte maksimumsbeløpet i henhold til artikkel 83 nr. 4, 2 % av den samlede årsomsetningen, som i 2023 utgjorde 1 609 040 000 kroner, eller ca. 143 146 000 euro.²⁶⁵

Vi viser til våre vurderinger ovenfor om faktorene i personvernforordningen artikkel 83 nr. 2 bokstav a–k. Det er svært viktig at en behandlingsansvarlig opprettholder god internkontroll, gjennomfører nødvendige vurderinger som dokumenteres og etablerer nødvendige organisatoriske tiltak, noe vi har funnet at manglet i tilsynsperioden. Det legges også vekt på Telenor ASAs uaktsomhet (artikkel 83 nr. 2 bokstav b), særlig med tanke på selskapets størrelse og innflytelse og hva som er forventet av et slikt selskap.

Når det har sagt, har vi ikke funnet noen direkte skade på de registrerte. Dette er en faktor som veier tungt i denne saken. Vi har dessuten lagt stor vekt på at saksbehandlingstiden har vært lang og at det har vært liggetid, noe som tilsier at beløpet bør nedjusteres. Dette er også i samsvar med praksis hos Personvernemnda, se avgjørelser i sakene PVN-2022-3, PVN-2021-20, PVN-2021-16, PVN-2021-13 og PVN-2021-3.

I sum mener vi derfor at overtredelsesgebyret bør settes lavt.

Vi mener at et overtredelsesgebyr på 4 000 000 NOK, eller ca. 0,005 % av Telenor Groups årsomsetning for 2023, står i et rimelig forhold til overtredelsen og virker avskrekkende i denne saken, i lys av de konkrete omstendighetene. Dette overstiger ikke det som er nødvendig for å oppnå etterlevelse av personvernforordningen i denne saken.

14 Inndrivelse av overtredelsesgebyr

Overtredelsesgebyret forfaller til betaling fire uker etter at vedtaket er endelig, jf. personopplysningsloven (2018) § 27. Vedtaket er tvangsgrunnlag for utlegg. Inndrivelse av kravet vil bli gjennomført av Statens innkrevingsentral.

15 Europeisk samarbeid

Dette vedtaket er fattet i samarbeid med de andre berørte tilsynsmyndighetene, i henhold til personvernforordningen artikkel 60.

²⁶³ I tidligere tilsendt engelskspråklig varsel ble årsrapporten for 2022 lagt til grunn fordi årsrapporten for 2023 ikke var publisert. Varselet er oppdatert med informasjon fra årsrapport 2023.

²⁶⁴ Basert på omregningskursen mellom euro og norske kroner per 29. desember 2023 på 11,2405 ifølge Norges Bank: [Valutakurser \(norges-bank.no\)](https://www.norges-bank.no/valutakurser), sist besøkt 11. april 2024.

²⁶⁵ Basert på omregningskursen mellom euro og norske kroner per 29. desember 2023 på 11,2405 ifølge Norges Bank: [Valutakurser \(norges-bank.no\)](https://www.norges-bank.no/valutakurser), sist besøkt 11. april 2024.

16 Adgang til dokumenter

I henhold til forvaltningsloven §§ 18 og 19 har Telenor ASA – som part i denne saken – rett til å gjøre seg kjent med sakens dokumenter. Dokumenter i saken ble oversendt 22. desember 2021 og 22. mars 2024.

I henhold til offentlighetsloven § 3²⁶⁶ er alle våre saksdokumenter som hovedregel åpne for innsyn. Dersom dere mener at noen av dokumentene i denne saken bør være helt eller delvis unntatt offentligheten basert på rettslige unntak, ber vi dere melde fra til oss og oppgi begrunnelse for kravet.

17 Klageadgang

Når et vedtak er truffet i henhold til personvernforordningen artikkel 56 nr. 2 og kapittel VII, kan det bringes inn for Oslo tingrett i medhold av personvernforordningen artikkel 78 nr. 1, personopplysningsloven §§ 22 og 25 og tvisteloven § 4-4 nr. 4.²⁶⁷

Med vennlig hilsen

Mona Naomi Lintvedt
stedfortredende direktør

Anna Kristin Ulfarsdottir
juridisk fagdirektør

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer

²⁶⁶ Lov av 19. mai 2006 nr. 16 om rett til innsyn i dokument i offentlig verksemd (offentleglova)

²⁶⁷ Lov av 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven).