Datatilsynet

POSTNORD AS
Postboks 6441 Etterstad
0605 OSLO

Deres referanse	Vår referanse	Dato
	20/02144-16	09.01.2023

Vedtak om pålegg - PostNord AS

1 Innledning

Vi viser til varselet om pålegg av 25. mai 2022 og merknadene deres av 25. august 2022.

Vi forstår merknadene slik at PostNord AS aksepterer det varslede pålegget, og at selskapet planlegger å innføre tofaktorautentisering ved hjelp av personlig passord og engangskode på SMS for å sikre konfidensialiteten i «mypostnord».

På bakgrunn av merknadene deres fatter vi vedtak i tråd med varselet.

2 Vedtak

> *Med hjemmel i personvernforordningen artikkel 58 nr. 2 bokstav d pålegges POSTNORD AS, org.nr. 984 054 564, å gjennomføre egnede tekniske tiltak for å oppnå et egnet beskyttelsesnivå som sikrer konfidensialiteten i tjenesten «mypostnord», jf. personvernforordningen artikkel 32 nr. 1 og nr. 2.*

Fristen for å gjennomføre påleggene fremgår av vedtakets pkt. 7.

3 Nærmere om sakens faktiske forhold

Sakens bakgrunn er to meldinger om brudd på personopplysningssikkerheten fra POSTNORD AS («PostNord»).

Meldingen av 24. februar 2020 (dok.nr 20/00643-1) gjelder en person som har overtatt et mobiltelefonnummer og dermed fikk tilgang til tidligere eier av nummeret sin kundeprofil hos POSTNORD («Melding 1»).

Meldingen av 6. mars 2020 (dok.nr 20/00799-1) gjelder en kunde hos POSTNORD som ved registrering tastet feil mobilnummer. All etterfølgende informasjon ble deretter sendt til dette mobilnummeret, og eieren av det feiltastede mobilnummeret fikk tilgang til hele kundeprofilen («Melding 2»).

Ettersom begge meldingene gjelder uautorisert tilgang til kundeprofiler behandler vi meldingene samlet.

Dere forklarer i meldingene at tilgang til kundeprofiler innebærer tilgang til kundens navn, kjønn, fødselsdato, postadresse, e-postadresse, telefonnummer, ordre- og betalingshistorikk, samt oversikt over sendinger underveis og avsendernavn. I tillegg gir tilgang til en kundeprofil mulighet til å endre varslingsinnstillinger.

I meldingen av 24. februar fremgår det at bruddet pågikk mellom 31. mars 2017 og 21. februar 2020. I meldingen av 6. mars fremgår det at bruddet pågikk mellom 8. august 2019 og 6. mars 2020.

Datatilsynet har ved to anledninger bedt PostNord redegjørelse for sakens faktiske forhold, herunder for risikovurdering av og sikkerheten i tjenesten mypostnord, samt for plasseringen av behandlingsansvaret i PostNord-konsernet.

I tillegg til meldingene fra PostNord og selskapets redegjørelser, har Datatilsynet mottatt tips fra brukere som har opplevd å få tilgang til andre brukeres personopplysninger.

I merknadene til varselet skriver PostNord at selskapet tar varselet om pålegg til etterretning, og at selskapet nå har gjennomført en risikovurdering og identifisert egnede tiltak for å sikre konfidensialiteten i tjenesten mypostnord.

4 Regelverkets krav

4.1 *Behandlingsansvarlig*

Den «behandlingsansvarlige» er den som bestemmer formålet med behandlingen og hvilke midler som skal benyttes, jf. personvernforordningen artikkel 4 nr. 7.

4.2 Grunnleggende prinsipper for behandling av personopplysninger

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

> *1. Personopplysninger skal*
>
> *a) behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»),*
>
> *b) samles inn for spesifikke, uttrykkelig angitte og berettigede formål og ikke viderebehandles på en måte som er uforenelig med disse formålene (...) («formålsbegrensning»),*

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

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

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

4.3 Sikkerhet ved behandlingen

Personvernforordningen artikkel 32 oppstiller krav til sikkerhet rundt behandling av personopplysninger:

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

a) pseudonymisering og kryptering av personopplysninger,

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

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

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

5 Datatilsynets vurdering

5.1 Behandlingsansvarlig

På bakgrunn av informasjonen PostNord har sendt oss legger vi til grunn at selskapet PostNord AS er behandlingsansvarlig for behandlingen av personopplysninger gjennom tjenesten mypostnord, jf. personvernforordningen artikkel 4 nr. 7.

5.2 Sikkerhet ved behandlingen

«mypostnord» er ifølge PostNord en tjeneste laget for privatkunder som bruker selskapets spedisjonstjenester. Formålet med tjenesten er å gi kunden en oversikt over sendinger på vei til eller fra dem:

> *Hensikten med MyPostNord for privatmottakere, er å gi forbrukere en egen, privat flate mot PostNord, hvor de kan få informasjon om sine sendinger, og tilpasse sin levering gjennom å gjøre endringer på sendinger som er på vei til seg.*

Bakgrunnen for denne saken er to meldinger om brudd på personopplysningssikkerheten fra PostNord, der nye brukere har fått tilgang til tidligere brukeres personopplysninger. Dette skjedde fordi de nye brukerne hadde fått tildelt telefonnumre som tidligere tilhørte andre brukere hos PostNord. Datatilsynet har også mottatt tips fra personer som har opplevd å få tilgang til andre brukeres personopplysninger i mypostnord.

PostNord forklarer hendelsene selskapet har meldt inn slik:

> *Tilgang til «tidligere eiers» profil vil kunne skje dersom mobilnummer skifter eier hos teleoperatør, og «tidligere eier» av telefonnummeret har ikke slettet sin profil hos PostNord før bytte av telefonnummer eller det har ikke gått minst 2 år fra «tidligere eier» sier opp sitt nummer hos teleoperatør til «ny eier» blir tilordnet nummeret fra teleoperatør. «Ny eier» vil da kunne logge seg inn på profil knyttet til telefonnummeret (siden dette verifiseres gjennom SMS som «ny eier» kan motta, og vil da ikke bli bedt om å lage ny profil hos PostNord.*
>
> *For teleoperatørene er det for øvrig praksis at telefonnummer som blir tilgjengelige, bl.a. fordi abonnementer sies opp, ikke overføres fra til ny eier før det er gått tre måneder nettopp for å sikre at nye eiere får henvendelser som gjelder tidligere eier som er situasjonen her. Unntaket er ved direktesalg av telefonnummer mellom to personer, dvs. «tidligere eier» og «ny eier», hvor man går utenfor systemet til teleoperatørene, se sak 2 nedenfor. «Tidligere eier» har i dette tilfellet ikke oppdatert tjenestene innenfor denne perioden. Tidligere forsendelser er heller ikke tilgjengelig i profil denne prosedyren om å ikke overføre telefonnummer etter minimum tre måneder, siden forsendelser slettes i profilen etter 14 dager.*
>
> *Årsaken til at «ny eier» vil få tilgang til profilen, er at «tidligere eier» f.eks. ikke har oppdatert profilen sin med sitt nye telefonnummer i nettbutikk som foretar forsendelser gjennom PostNord og/eller i profilen hos PostNord eller at «gammel eier» ved en forglemmelse oppgir sitt tidligere telefonnummer ved bestilling i nettbutikk. Nettbutikken vil da benytte det tidligere nummeret til «tidligere eier» ved forsendelse til «ny eier», og «ny eier» vil da motta varsel med forsendelse fra PostNord med link til profil hos PostNord. Legger derimot «tidligere eier» inn sitt nye telefonnummer ved bestilling eller har oppdatert sin profil, vil ikke forholdet oppstå, og det kan være noe av grunnen til at slike hendelser skjer meget sjeldent.*

> *«Ny eier» er ikke nødt til å gå inn på profilen for å få informasjon om forsendelser (SMSen opplyser om navn på mottaker, avsender (bedrift) og hentested, eller for å motta pakker. Men «ny eier» kan da velge selv å eventuelt å gå inn på profilen. Dette til tross for at vedkommende er klar over at SMSen ikke er til denne, siden det fremkommer av SMSen av hvem som er mottaker. «Ny eier» har dermed aksessert en profil denne vet vedkommende ikke har rett til å aksessere.*

Personvernforordningen artikkel 32 krever at den behandlingsansvarlige gjennomfører tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet med hensyn til risikoen.

Spørsmålet i vår sak er om beskyttelsesnivået i mypostnord er egnet med hensyn til risikoene ved behandling av personopplysninger i systemet, herunder om dagens beskyttelsesnivå i tilstrekkelig grad sikrer vedvarende konfidensialitet rundt personopplysningene i systemet, jf. artikkel 32 nr. 1 bokstav b.

Risikoene for fysiske personers rettigheter og friheter

Før vi vurderer om dagens beskyttelsesnivå er egnet, vil vi si noe om risikoene for de registrertes rettigheter og friheter knyttet til behandlingen av personopplysninger i mypostnord.

Ifølge artikkel 32 nr. 1 og nr. 2, skal den behandlingsansvarlige gjennomføre egnede tekniske tiltak i sine behandlingssystemer med utgangspunkt i risikoene forbundet med behandlingen. Tiltakene skal blant annet ivareta «evne til å sikre vedvarende konfidensialitet» i den behandlingsansvarliges systemer og tjenester, jf. artikkel 32 nr. 1 bokstav b.

Ved vurderingen av hvilke tiltak som er egnet, skal den behandlingsansvarlige ta hensyn til den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, formål, og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for de registrertes rettigheter og friheter.

Som et første steg i å sikre et egnet sikkerhetsnivå, pålegger artikkel 32 nr. 1 den behandlingsansvarlige å identifisere risikoene knyttet til behandlingen av personopplysninger. Denne objektive vurderingen, gjerne kalt «risikovurdering», skal identifisere risikoene for fysiske personers rettigheter og friheter. Risikoene den behandlingsansvarlige identifiserer gjennom vurderingen er styrende for hvilke tekniske og organisatoriske tiltak den behandlingsansvarlige må gjennomføre for å sikre et egnet beskyttelsesnivå, jf. artikkel 32 nr. 1 og nr. 2.

Fortalepunkt 76 til personvernforordningen sier følgende om vurderingen:

> *Hvor sannsynlig og alvorlig risikoen for den registrertes rettigheter og friheter er, bør fastslås ut fra behandlingens art, omfang, formål og sammenhengen den utføres i. Risikoen bør vurderes ut fra en objektiv vurdering der det fastslås om behandlingen av personopplysningene innebærer en risiko eller en høy risiko.*

(Vår utheving).

I vårt krav om redegjørelse ba vi PostNord om å sende oss selskapets risikovurdering for mypostnord og relaterte behandlingssystemer. PostNord viser i sin redegjørelse til dokumentet «Sikkerhetsvurdering MyPostNord».

PostNord har i det oversendte ikke dokumentert *når* vurderingen ble gjennomført.

For å kunne påvise at prinsippene etterleves, jf. art. 5 nr. 2, og for å kunne «*sikre og påvise at behandlingen utføres i samsvar med denne forordning*», jf. art. 24 nr. 1, er det nødvendig med en systematisk tilnærming til arbeidet med regeletterlevelse. PostNord må kunne påvise tidspunktet for vurderingen, blant annet slik at Datatilsynet kan kontrollere at den ble gjennomført før behandlingen av personopplysninger startet. Dette er ikke mulig utfra dokumentasjonen PostNord har oversendt.

Videre mangler den oversendte risikovurderingen en systematisk oversikt og vurdering av relevante risikoer knyttet til selskapets behandling av personopplysninger i tjenesten.

Personvernforordningen angir ingen metodikk for gjennomføring av risikovurderinger, men den behandlingsansvarlige må i lys an ansvarlighetsprinsippet ha en systematisk tilnærming til regeletterlevelsen, som gjør at den har dokumentert og kan påvise etterlevelse, jf. artikkel 5 nr. 2.

Den behandlingsansvarlige må minst kunne demonstrere at de har oversikt over relevante risikoer, at de har vurdert dem i tilstrekkelig grad og gjennomført egnede tiltak for å redusere risikoen for brudd på personopplysningssikkerheten. Vi kan ikke se at risikoen for at en bruker får personopplysningene sine på avveie via mypostnord er vurdert i tilstrekkelig grad i dokumentasjonen selskapet ha sendt oss. PostNord har heller ikke vurdert den særlige risikoen for konfidensialitetsbrudd som tjenesten innebærer for brukere som får nytt telefonnummer via direktesalg, hvor taushetsbelagt informasjon kan røpes for uvedkommende.

Den mest utbredte måten å gjennomføre risikovurderinger på er å liste opp aktuelle risikoscenarier og vurdere sannsynlighet og konsekvens for disse. Med grunnlag i den vurderingen avgjør man om risikoene er akseptable eller om det må gjennomføres tiltak. Dersom risikoene ikke er akseptable vurderer man ulike risikoreduserende tiltak og avgjør hvilke som er egnede. Deretter angir man hvem som skal gjennomføre de ulike tiltakene og fristen for gjennomføring. Vi anbefaler at PostNord tar i bruk en anerkjent metodikk for gjennomføring av risikovurderinger, for eksempel basert på ISO27001.

Vår foreløpige vurdering er at risikovurderingen PostNord har sendt oss ikke i tilstrekkelig grad identifiserer risikoene knyttet til selskapets behandling av personopplysninger i mypostnord. Vurderingen har sentrale mangler som gjør den uegnet til å identifisere risikoene ved behandlingen slik artikkel 32 nr. 1 og nr. 2 krever.

I det følgende vil vi si noe overordnet om risikoen for de registrertes rettigheter og friheter ved bruk av mypostnord, ettersom risikoene er styrende for hvilke tekniske tiltak PostNord som behandlingsansvarlig må gjennomføre i tjenesten.

Ifølge PostNord lagres følgende informasjon i en kundeprofil i mypostnord:

- Fornavn, etternavn, mobilnummer, e-post, bilde, fødselsdato og kjønn (der de tre siste ikke kreves fylt inn, og blir sjeldent fylt inn av brukerne).
- Adresse
- Pakker på vei med navn på avsender (bedriftsnavn). Denne informasjonen beholdes kun i 14 dager i arkivet i profilen.
- Varslingsinnstillinger, dvs. hvilke varsler vedkommende ønsker å motta fra PostNord, som epost eller SMS.
- Bedriftsmottakere eller avtalekunder man er tilknyttet (og administrasjon av disse om rollen tilsier det).
- Hvilke typer adviseringer (dvs. varsel om mottak av forsendelse) som er sendt når, kanal og status (men ikke innhold).
- Betalingshistorikk (datotid, type, sendingsnummer, beløp, status, betalingsmåte, referanse og transaksjonsidentifikator). Dette er kun data mot PostNord dersom det er kjøpt tilleggstjenester hos PostNord, som Flex dvs. endret utleveringssted (men står da kun «Flex» i profilen), egen forsendelse (står da kun «Mypack GO») eller oppkrav (står da kun «CashOnDelivery»). Betalingshistorikk kan være slettet av bruker.
- PostNord Pluss nivå, om man er medlem av PostNord, som angir kun hvor mange pakker som er sendt fra PostNord og hvilket brukernivå man da er på («Gold», «Silver» eller «Basic»), men ingen informasjon om pakker mv.

Disse opplysningene er i utgangspunktet ikke særlige kategorier av personopplysninger etter personvernforordningen artikkel 9.

Opplysningene kan imidlertid fortsatt være av sensitiv karakter for de registrerte, og dette gjelder særlig sendingshistorikken med informasjon av navn på avsender. PostNord har en stor markedsandel i Norden, og brukes av mange ulike typer nettbutikker, herunder apotek.[1]

PostNord er ikke bare omfattet av bestemmelsene i personvernforordningen, men også postloven. Det angis i postloven § 30 at tilbyder av posttjeneste har taushetsplikt for:

> *[…] informasjon om avsender og mottakers bruk av posttjeneste, […] avsender og mottakers forretningsmessige eller personlige forhold og […] innhold i postsending».*

Ifølge postloven er tilbyderen forpliktet til å «gjennomføre tiltak for å hindre at uvedkommende får kjennskap til informasjonen». Datatilsynet er ikke tilsynsmyndighet for

[1] Se for eksempel nettbutikkene til Apotek 1, Boots Apotek, Vitusapotek og Farmasiet.no, https://www.apotek1.no/kundesenter/frakt-og-levering, https://www.boots.no/frakt-og-levering, https://www.vitusapotek.no/kundeservice/levering-og-betaling/a/A1361, https://www.farmasiet.no/kundesenter/frakt-og-levering (sist besøkt 25.05.22).

postloven, men bestemmelsen om taushetsplikt er likevel egnet til å si noe om sensitiviteten for opplysningene som denne saken gjelder.

Vi bemerker også at fysiske personers korrespondanse er i kjernen av retten til privatliv etter den europeiske menneskerettighetskonvensjon artikkel 8.

Integritet- og konfidensialitetsprinsippet er et grunnleggende prinsipp for behandling av personopplysninger. jf. artikkel 5 nr. 1 bokstav f.

Tiltak for å oppnå et egnet sikkerhetsnivå med hensyn til risikoen

Det neste spørsmålet er om PostNord har gjennomført egnede tekniske tiltak som sikrer et egnet beskyttelsesnivå i mypostnord i lys av risikoene ved behandling av personopplysninger, jf. personvernforordningen artikkel 32 nr. 1.

PostNord anfører at de tekniske tiltakene som per i dag er innført i mypostnord oppfyller kravet til tekniske tiltak og sikrer et egnet sikkerhetsnivå etter artikkel 32:

> *Konfidensialitet er sikret ved at det kreves autentisering fra telefonnummer, se ovenfor, og at risikoen for tilgang ved skifte av telefonnummer er meget liten. I tillegg er det ikke er alternative tiltak som ville økt sikkerheten hensett personopplysninger som er tilgjengelig i løsningen og tilgjengelighet for brukerne, se nedenfor. Bruk av telefonnummer er også bransjestandard, og dette er også løsningen som bl.a. Posten benytter.*
>
> *Taushetsplikt etter postloven overholdes etter løsningen som er valgt, og det vil ikke være løsninger eller tiltak som gir mer sikkerhet. Tidligere ble varsel om pakke sendt ut per post i postkassen, og slik løsning gir mindre sikkerhet (pga. de fleste ikke har låste postkasser) enn løsningen som nå benyttes.*
>
> *Det skal også presiseres at gitt sikkerhetsnivået som nevnt, så skyldes hendelsen den registrertes eget forhold, samt at mottakeren av SMS-varsling («ny eier») har handlet mot bedre vitende, dersom vedkommende har gått inn på tidligere eiers profil.*

Per i dag bruker PostNord telefonnummer som identifikator for tilgang til tjenester og profiler hos selskapet:

> *Mobilnummer er brukt som identifikator for tilgang til tjenester og profiler hos PostNord som etter PostNords vurdering, se vedlagte risikovurdering, gir et tilstrekkelig sikkerhetsnivå og risikonivå hensett de opplysninger som behandles og som er tilgjengelig på mottakers (den registrertes) profil samt i SMS-varsel, at dette er begrensede opplysninger og ikke av sensitiv art eller særlige kategorier og at det er behov for å motta varsling om pakker raskt og enkelt, og tilsvarende for tilgang til egen profil og tjenestene der (art, omfang, formål og den sammenheng de utføres i), se også nedenfor, tilgjengelighet for tjenestene (brukervennlighet), det nivå på sikkerhet som er tilgjengelig og praksis for slik informasjon og tjenester (den tekniske*

utviklingen), gjennomføringskostnadene (som at dette er en mer kostbar løsning enn epost (en kostnad på ca. kr 2,6 millioner per år, men BankID er en meget kostbar løsning, med ca. kr 10,8 millioner per år).

(Vår utheving)

Vi er uenig i denne vurderingen.

Vårt syn er at autentiseringen av brukere i mypostnord kun med bruk av telefonnummer ikke sikrer et egnet beskyttelsesnivå som sikrer konfidensialiet i tjenesten, jf. personvernforordningen artikkel 32 nr. 1 bokstav b.

For det første innebærer dagens ordning med telefonnummer som eneste autentisering at personer som kjøper telefonnummer via direktesalg, og som besøker mypostnord, vil få tilgang til den tidligere eierens personopplysninger, inkludert sendingsinformasjon.

PostNord anfører at sendingsinformasjonen kun lagres i 14 dager, og at konfidensialiteten for denne informasjonen kun kan brytes dersom et telefonnummer bytter eier gjennom en direktetransaksjon, hvor telefonnummeret ikke omfattes av teleoperatørenes karantenetid.

PostNord er kjent med at det foregår direktesalg av telefonnumre i Norge, og at dette ikke er ulovlig, selv om det foregår i mindre utstrekning enn tildeling av telefonnumre fra teleoperatørene. Ettersom telefonnumre er en begrenset ressurs, og vi stadig blir flere i Norge, følger det logisk at det vil være økende sannsynlighet for lignende tilfeller av konfidensialitetsbrudd i fremtiden. Hvis markedsandelen til PostNord øker i Norge vil sannsynligheten øke ytterligere.

For det andre innebærer dagens ordning at personer som får tildelt et nytt telefonnummer fra en teleoperatør, vil få tilgang til personopplysningene til den tidligere eieren av telefonnummeret, når den nye eieren bruker mypostnord.

PostNord er etter personvernforordningen videre forpliktet til å sikre konfidensialiteten til alle personopplysninger det behandler som behandlingsansvarlig.

Etter at sendingsinformasjon er slettet etter 14 dager lagrer mypostnord de øvrige personopplysningene i ett år før de slettes. Ettersom karantenetiden for gjenbruk av telefonnumre som distribueres via teleoperatørene er mindre enn ett år, er det mye høyere sannsynlighet for at konfidensialiteten brytes for disse opplysningene. Argumentene om telefonnumre som begrenset ressurs og potensiell økning i PostNord sin markedsandel er enda mer aktuelle her.

PostNord anfører selv at «Opplysningene […] er grunnleggende informasjon som er nødvendig for mottakere fra PostNord, og ikke å anse som sensitive eller inngripende for mottakeren». Dette er neppe et gyldig argument for alle brukere, og uansett ikke noe fripass for å tillate konfidensialitetsbrudd, selv om dette gjelder et fåtall brukere.

Vår vurdering er at med dagens beskyttelsesnivå vil uvedkommende med jevne mellomrom få tilgang til brukeres personopplysninger i mypostnord.

Vi bemerker at ansvaret for å sørge for personopplysningssikkerheten etter personvernforordningen ligger hos den behandlingsansvarlige, og at PostNord ikke kan skyve dette ansvaret over på sluttbrukeren med argumentet om at en bruker med nytt telefonnummer burde forstått at den var i ferd med å få tilgang til andres personopplysninger og dermed «handler mot bedre vitende».

På bakgrunn av dette er vår vurdering er at PostNord ikke har gjennomført egnede tekniske tiltak for å oppnå et egnet beskyttelsesnivå i tjenesten mypostnord. Selskapet har ikke gjennomført egnede tiltak som sikrer vedvarende konfidensialitet i tjenesten.

Vår konklusjon er dermed at PostNord har brutt personvernforordningen artikkel 32.

6 Vurdering av korrigerende tiltak

Vår vurdering er at PostNord ikke har gjennomført egnede tekniske tiltak som sikrer et egnet beskyttelsesnivå og konfidensialitet i mypostnord, jf. personvernforordningen artikkel 32 og artikkel 5 nr. 1 bokstav f, slik tjenesten er utformet i dag.

Vi anser det derfor nødvendig å pålegge PostNord å gjennomføre tekniske tiltak for å sikre et tilstrekkelig beskyttelsesnivå og ivareta konfidensialiteten i mypostnord.

Pålegget innebærer for det første at PostNord må identifisere risikoene knyttet til behandlingen av personopplysninger i mypostnord i tråd med artikkel 32 nr. 1 og nr. 2, jf. fortalepunkt 76.

Videre innebærer pålegget at PostNord må iverksette egnede tekniske tiltak for å sikre et egnet beskyttelsesnivå og konfidensialitet i mypostnord. Selskapet må iverksette tiltak som forhindrer at personer som får nytt telefonnummer gjennom direktesalg eller tildeling fra en teleoperatør får uautorisert innsyn i andre brukeres personopplysninger hos PostNord.

I merknadene til varselet skriver PostNord følgende:

> *PostNord har på bakgrunn av denne saken gjennomført en risikovurdering (se vedlagt bilag). I risikovurderingen har vi kartlagt risikoen vi oppfatter som aktuell, i tillegg til å identifisere egnet teknisk- og organisatorisk risikoreduserende tiltak. PostNord har vurdert at risikoen vil bli redusert betraktelig ved innføring av egnet tiltak.*
>
> *For å tilfredsstille PostNord egne målkrav til forsvarlig sikkerhet, så har PostNord besluttet å innføre ytterlige krav til innlogging i MyPostNord - applikasjonen. PostNord har vurdert det slik at innføring av to-faktoridentifisering vil heve sikkerhetsnivået i MyPostNord. Dette vil innebære at man innfører personlig passord i tillegg til dagens løsning med kode på SMS. Videre anses*

sannsynligheten for at uvedkommende får tilgang til systemet som ubetydelig (forutsatt at man ikke har tilgang til det personlige passordet eller SMS-kode).

Vi pålegger som nevnt i varselet ikke PostNord å gjennomføre bestemte tekniske tiltak for å oppnå et egnet sikkerhetsnivå og konfidensialitet. Dette fordi det er selskapets oppgave å selv identifisere egnede tekniske tiltak i lys av den identifiserte risikoen for fysiske personers rettigheter og friheter som oppstår ved behandling av personopplysninger i tjenesten.
Vi nevner likevel at vi er enige i at de beskrevne tiltakene vil være en hensiktsmessig måte å sikre konfidensialiteten i mypostnord på.

Vår hjemmel for å pålegge selskapet å gjennomføre egnede tekniske tiltak for å oppnå et egnet beskyttelsesnivå og konfidensialitet er personvernforordningen artikkel 58 nr. 2 bokstav d.

7 Klagerett og videre saksgang

Dere kan klage på vedtaket. En eventuell klage må sendes til oss **innen tre uker** etter at dette brevet er mottatt, jf. forvaltningsloven §§ 28 og 29. Dersom vi opprettholder vårt vedtak vil vi sende saken videre til Personvernnemnda for klagebehandling.

Fristen for å gjennomføre pålegget er **4 uker** etter klagefristens utløp. Dersom dere ikke påklager pålegget må dere innen denne fristen sende oss en skriftlig bekreftelse, samt dokumentasjon, på at pålegget er gjennomført.

8 Offentlighet, innsyn og taushetsplikt

Vi vil informere dere om at alle dokumentene i utgangspunktet er offentlige, jf. offentlighetsloven § 3. Dersom dere mener det er grunnlag for å unnta hele eller deler av dokumentet fra offentlig innsyn, ber vi dere om å begrunne dette.

Datatilsynet har taushetsplikt om hvem som har varslet oss om brudd på personopplysningsloven med personvernforordningen, og om deres personlige forhold. Taushetsplikten følger blant annet av personopplysningsloven § 24 og forvaltningsloven § 13. Som part i saken kan dere likevel bli gjort kjent med slike opplysninger av Datatilsynet, jf. forvaltningsloven § 13 b første ledd nr. 1. Dere har også rett til innsyn i sakens dokumenter, jf. forvaltningsloven § 18.

Vi gjør oppmerksom på at dere har taushetsplikt om opplysninger dere får av Datatilsynet om identiteten til personer som varsler om brudd på personopplysningsloven med personvernforordningen, personlige forhold og andre identifiserende opplysninger, og at dere bare kan bruke disse opplysningene i den utstrekning det er nødvendig for å ivareta interessene deres i denne saken, jf. forvaltningsloven § 13 b andre ledd. Vi gjør også oppmerksom på at brudd på denne taushetsplikten kan straffes etter straffeloven § 209.

Hvis dere har spørsmål om saken, kan dere ta kontakt på e-post omm@datatilsynet.no eller telefon 22 39 69 59.

Med vennlig hilsen

Ylva Marrable
seksjonssjef

Ole Martin Moe
juridisk seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen håndskrevne signaturer