ÅRSRAPPORT 2021

PERSONVERN

INNHOLDSFORTEGNELSE

1. INNLEDNING

1.1 BAKGRUNNEN FOR DENNE RAPPORTEN

Vi har alle noe vi ikke vil dele med andre. Ikke fordi det er ulovlig eller noe vi må skjule, men fordi det rett og slett er privat. Personvern handler om vern av personopplysninger, og retten til å få ha privatlivet sitt i fred. Det ideelle er at den enkelte skal ha kontroll over, og i størst mulig grad kunne bestemme over, egne personopplysninger. Alle mennesker har en ukrenkelig egenverdi.

I personvernforordningen er det lovfestet at personvernombudet, heretter også omtalt som ombudet, skal rapportere direkte til det høyeste ledelsesnivået for å sikre sin uavhengighet fra den øvrige linjeorganisasjonen, jf. personvernforordningen art. 38 nr. 3. Denne artikkelen i forordningen ligger som utgangspunkt for denne rapporten. I tillegg er det vurdert at en årsrapport også er nyttig for å belyse status på området. Det er nødvendig å få formidlet gjeldende status på personvern.

I denne årsrapporten er det sammenstilt elementer som allerede er på plass ved 31. desember 2021, og de mest sentrale oppgavene som skal gjennomføres i 2022. Rapporten kan på denne bakgrunn være til hjelp for å finne ut av hva som fortsatt gjenstår for å oppnå fullstendig etterlevelse av gjeldende lovverk.

I tillegg skal rapporten belyse noen erfaringer som personvernombudet gjorde seg i sitt påbegynnende arbeid. Disse erfaringene har ført til noen endringer som vil bli konkretisert i punkt 3.2.1.

2. PERSONVERN

2.1 NYTT REGELVERK

I 2018 vedtok Stortinget en ny personopplysningslov. Denne loven består av våre nasjonale paragrafer, men også EUs personvernforordning (GDPR). Vi har inkorporert GDPR i norsk rett, som betyr at GDPR gjelder som norsk rett.

Før Stortinget vedtok den nye personopplysningsloven fra 2018 hadde vi en eldre personopplysningslov. Den nye personvernforordningen (GDPR) erstattet personvern-direktivet 95/46/EF som var inntatt i EØS-avtalen og gjennomført i den tidligere personopplysningsloven. Personvern har altså eksistert lenge, men det er først nå i nyere tid at det har fått et annet fokus.

Forordningsformen fører til full harmonisering av personvernreglene i EU/EØS. Dette innebærer at det i utgangspunktet ikke er adgang til å fravike reglene og heller ikke til å gi supplerende regler. Imidlertid åpner forordningen selv for at det kan gis nasjonale regler i enkelte tilfeller. Regelverket om personvern gir private/borgere noen rettigheter, samtidig som det også gir det offentlige noen plikter. Fordi Alta kommune er et offentlig forvaltningsorgan med over 250 ansatte tillegger GDPR oss noen plikter. Noen av disse pliktene vil bli belyst i rapporten.

3. VIRKSOMHETENS PLIKTER

3.1 PERSONVERNOMBUD

I 2021 ble det ansatt et personvernombud i Alta kommune, og Frida Eilertsen begynte 1. september i stillingen som personvernombud. Personvernombudet skal foreta noen lovpålagte oppgaver, herunder blant annet ha ansvar for at Alta kommune har kontroll på alle gangene man behandler personopplysninger. Det skal føres en protokoll over alle disse behandlingsaktivitetene. Det blir foretatt en nærmere beskrivelse av dette i punkt 3.2. I tillegg skal ombudet bidra til kompetanseheving og utvikling av personvern- og sikkerhetskultur i kommunen. Videre skal personvernombudet opptre som en rådgiver for kommunens ledelse og ansatte innen personvern og informasjonssikkerhet, så personvernombudet skal bistå i både små og store utfordringer. Dette er kanskje personvernombudets viktigste oppgave. Personvernombudet skal være et verktøy slik at den behandlingsansvarlige best mulig kan ivareta personverninteressene.

En annen oppgave som er lagt til personvernombudet er at det skal være med å etablere rutiner og interne retningslinjer. Når det gjelder dette punktet anses det som nødvendig at personvernombudet først foretar en kartlegging av de rutinene og interne retningslinjene som allerede foreligger og er etablert før det nedsettes nye rutiner og retningslinjer. En nærmere beskrivelse av dette vil fremgå videre i rapporten.

I tillegg til de nevnte oppgaver skal personvernombudet også gi uttalelser vedrørende personvernkonsekvenser. Denne oppgaven er påbegynt, og vil også belyses nærmere i rapporten. En ny plikt etter det nye regelverket er at det skal gjennomføres personvernkonsekvensvurderinger. Personvernombudet vil ha ansvar for å kontrollere gjennomføringen av disse konsekvensvurderingene. En nærmere beskrivelse av dette vil fremkomme i punkt 3.4.

Videre skal personvernombudet være med på å sikre at regelverket overholdes. Denne overordnede oppgaven må ivaretas gjennom alt arbeid som skal utføres. Selv om personvernombudet har et særskilt ansvar for at regelverket overholdes har alle ansatte og ledere i Alta kommune likevel et ansvar for å ivareta personvernet i det arbeidet som gjøres daglig. Selv om en virksomhet har personvernombud, er det fremdeles den behandlingsansvarlige som har det juridiske ansvaret for at personvernlovgivningen følges.

Personvernombudet skal samarbeide med Datatilsynet og fungere som et kontaktpunkt for tilsynet ved eventuelle spørsmål. Ved behov skal ombudet også kunne rådføre seg med tilsynet. Ombudet skal legge til rette for at Datatilsynet får den informasjonen de trenger for å utføre sine oppgaver og plikter, for eksempel i forbindelse med sin kontrollvirksomhet.

De registrerte (for eksempel innbyggere og ansatte) skal kunne kontakte personvernombudet med alle spørsmål knyttet til behandling av deres opplysninger, og om utøvelsen av rettighetene de har i henhold til personvernlovgivningen. Dette vil belyses nærmere i punkt 3.6.

3.2 OVERSIKT OVER BEHANDLINGER I VIRKSOMHETEN – BEHANDLINGSPROTOKOLL

Som følge av det nye regelverket har Alta kommune blitt tillagt noen plikter, herunder blant annet å ha en oversikt over alle gangene vi behandler/registrerer/overfører/sletter personopplysninger. Dette gjelder for alle tjenesteområder. Hver gang noen eksempelvis sender byggesøknad, meldes inn på skole, er i kontakt med barneverntjenesten, og får lønn fra Alta kommune, så behandler vi personopplysninger.

Vi skal altså utarbeide en oversikt over alle gangene vi behandler personopplysninger. Oppgaven er lovpålagt, og påbegynt på noen tjenesteområder. Det gjenstår dog mye arbeid. Dette skal være ferdigstilt i 2022. Oppgaven er delt i to deler, der den ene består av å kartlegge behandlingsaktiviteter, mens den andre delen består av å sjekke og kontrollere at regelverket overholdes. For å få kartlagt risikobildet når det kommer til personvern må det foretas personvernkonsekvensvurderinger. For å foreta personvernkonsekvensvurderinger må man ha et skjema for å kunne gjøre dette. Innen 2022 skal skjemaet for å kunne gjennomføre personvernkonsekvenser være ferdigstilt. I forlengelse av dette vil det da være mulig å få en bredere oversikt over risikobildet, og da også se og kartlegge høyrisikoområdene. Når vi får kartlagt høyrisikoområdene, kan vi begynne å gjennomføre tiltak for å minke risikoen.

En behandling av personopplysninger kalles behandlingsaktivitet. Disse behandlingsaktivitetene skal registreres i det vi kaller behandlingsprotokoll. En behandlingsprotokoll er altså en oversikt over alle gangene en virksomhet behandler personopplysninger. Personvernregelverket oppstiller noen krav til hva en slik oversikt må inneholde:

1) Behandlingsansvarliges navn og kontaktopplysninger, og navn og kontaktopplysninger til personvernombudet.
2) Formålet med behandlingen av personopplysningene.
3) En beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger.
4) Kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, herunder mottakere i tredjestater eller internasjonale organisasjoner.
5) Dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredjestat eller internasjonale organisasjon og, ved overføringer nevnt i artikkel 49 nr. 1

annet ledd, dokumentasjon på nødvendige garantier.

6) Dersom det er mulig, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger.
7) Dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1.

Å ha med disse oppstilte punktene anses som et minimumskrav i en behandlingsprotokoll. Måten en virksomhet velger å organisere og kartlegge behandlingsaktivitetene sine varierer ut i fra eksempelvis virksomhetens størrelse, antall ansatte, antall tjenesteområder, antall avdelinger/fagområder, mm. Noen virksomheter velger å anvende ferdige skjemaer i eksterne systemer, som hjelpemidler for å forenkle prosessen, mens andre velger å utarbeide egne skjemaer i Excel. Noen virksomheter velger å ha en behandlingsprotokoll med mange vedlegg, mens andre virksomheter velger å ha mange behandlingsprotokoller. Det er opptil hver enkelt virksomhet hvordan denne kartleggingen skjer. En kommune vil normalt ha mellom 200 og 500 protokoller/vedlegg. Alt ettersom hvordan man organiserer det. Enhver/ethvert protokoll/vedlegg vil inneholde en liste over behandlingsaktiviteter.

Med fremtiden kommer økt digitalisering, og med en økende digitalisering blir behovet for kontroll og oversikt viktigere.

3.2.1 STATUS

Å kartlegge alle gangene en kommune behandler personopplysninger anses som en omfattende oppgave, ettersom det innbefatter alle tjenesteområder, virksomheter og avdelinger. Arbeidet med å nedtegne en slik oversikt ble påbegynt i systemet Samsvar, tidligere Sureway, i 2018, og har siden da ikke vært jobbet med. Utgangspunktet er at personvernombudet har ansvaret for kartleggingen av behandlingsaktiviteter, men at det er lederne (kommunalledere, virksomhetsledere, avdelingsledere) som skal gjøre det. For å kunne starte prosessen med det videre arbeid var det derfor nødvendig å få kartlagt og analysert det som allerede var registrert. Det neste steget ble å vurdere hvorvidt det registrerte oppfylte kravene etter gjeldende lovverk.

Resultatet av denne første kartleggingen ble mitt utgangspunkt for videre arbeid: Omtrent en sjettedel av protokollene/vedleggene var påbegynt. Ved en nærmere granskning oppdaget ombudet at det var blitt gjort en del feil i registreringen. De fleste feilene som var gjort var at det hadde blitt registrert at Alta kommune i mange situasjoner behandler *sensitive* personopplysninger når man jamfør loven behandlet vanlige personopplysninger. Mange tenker at blant annet fødselsnummer anses som en sensitiv personopplysning når fødselsnummer egentlig er en alminnelig personopplysning. Sensitive personopplysninger er regulert i artikkel 9 i GDPR, der det står at:

«Behandling av personopplysninger om *rasemessig* eller *etnisk opprinnelse*, *politisk*

oppfatning, *religion*, *filosofisk overbevisning* eller *fagforeningsmedlemskap*, samt behandling av *genetiske opplysninger* og *biometriske opplysninger* med det formål å entydig identifisere en fysisk person, *helseopplysninger* eller opplysninger om en fysisk persons *seksuelle forhold* eller *seksuelle orientering*, er forbudt», jf. GDPR art. 9 første ledd.

Det krever altså særskilt hjemmel i lov for å behandle personopplysninger om rase, etnisitet, helse, seksuelle forhold mm., og det er ønskelig at den registrerte informasjonen er korrekt.

Med det overnevnte tatt i betraktning foretok personvernombudet en vurdering på om det var hensiktsmessig å først rette opp for så å fortsette registreringen i Samsvar. Etter en samlet vurdering fant ombudet ut, i samråd med leder, at arbeidet ikke skulle fortsettes i Samsvar. Videre plan for å kartlegge behandlingsaktivitetene var å rett og slett bruke Excel som verktøy. Behandlingsprotokoller anses som oppslagsverk for personvernombudet, og Datatilsynet dersom vi skulle bli gjenstand for kontroll. Det anses ikke som noe man trenger å anvende i arbeidshverdagen.

Etter en slik konklusjon startet arbeidet med å utarbeide Alta kommune sin egen protokoll for å registrere personopplysninger. Ved utarbeidelsen av denne er det sett hen til de krav som fremgår av loven, Datatilsynets tolkninger av lovkravene, andre kommuners maler til protokoller, og andre virksomheters maler til protokoller. I tillegg har ombudet brukt erfaring fra tidligere arbeidsplass. Alta kommunes mal for protokoll er ferdigstilt, og arbeidet med å registrere behandlingsaktiviteter er nå i gang. I protokollen skal man registrere følgende informasjon:

1) Type behandling (innsamle kontaktopplysninger, utlevere bilder til media, slette oppmøtestatistikk osv.)
2) Virksomhetsområde
3) Avdeling/fagområde (hvis relevant)
4) Formålet med behandlingen (utsende vielsesattester, behandle byggesøknad, utbetale lønn osv.)
5) Hvilket lovlig grunnlag vi har for å behandle personopplysningene (samtykke fra den registrerte, ved avtale, ved lov osv.)
6) Kategorier av registrerte (barn, foreldre, søkere osv.)
7) Kategorier personopplysninger (navn, fødselsdato, adresse, bilder osv.)
8) Kategorier sensitive/særlige personopplysninger hvis relevant (opplysninger om helse, seksualitet, religion osv.)
9) Kilde (om personopplysningene kommer fra personen selv, fra en forelder, fra en tredjeperson, innhentet fra et system osv.)
10) System (hvilket system personopplysningene behandles i)
11) Sletterutiner (om det finnes noen tidsfrist for sletting eller om registreringen av personopplysningene er arkivverdig)
12) Sikkerhet ved registreringen av personopplysningene (om det er nødvendig med anonymisering og kryptering, om man har evne til å sikre konfidensialitet osv.)
13) Databehandleravtaler (om vi har databehandleravtaler med systemet vi

behandler personopplysningene i, og hvor denne er lagret)

14) Overføring (om vi overfører personopplysningene til et land utenfor EU/EØS eller til internasjonale organisasjoner)

Malen til protokollen inneholder flere kategorier enn nødvendig, men erfaring tilsier at det etter hvert vil komme flere krav enn det som fremgår av regelverket slik det er nå. Malen som er utarbeidet skal være grei å fylle ut, og det skal ikke foretas unødvendig ressursbruk på det. En annen grunn til at det i malen er tatt med flere kategorier enn nødvendig er at personvernombudet finner det nyttig at Alta kommune selv skal ha kontroll på behandlingsaktiviteter og alle forhold knyttet til dette. Arbeidet med å overføre informasjon fra Samsvar til Excel er ferdigstilt, og avtalen med Samsvar er sagt opp. Dette utgjør en besparelse på 67 299, 75 kroner per år (pris for 2022).

I det videre arbeid framover skal resten av behandlingsaktivitetene kartlegges og fylles ut i Excel-dokumentet. Arbeidet anses som omfattende grunnet Alta kommunes store størrelse. På denne bakgrunn er det derfor viktig å ha en bred oversikt over virksomhetsområder, fagområder og avdelinger mm. En slik oversikt er nå utarbeidet, og står ferdigstilt og klar til disposisjon.

Det neste steget i en slik kartlegging er å ta kontakt med lederne, og forklare jobben som skal utføres. Det videre steget blir å sende ut Excel-skjemaet som skal utfylles, og veilede lederne ved behov. Dette arbeidet er påbegynt. Lederne kan til orientering delegere utfyllingen/kartleggingen videre, men det er nødvendig at lederne har kontroll på dette.

3.3 DATABEHANDLERAVTALER

Alle virksomheter som benytter seg av leverandører som behandler personopplysninger på vegne av virksomheten (behandlingsansvarlig) har plikt til å utarbeide en databehandleravtale. Databehandleravtalen skal sikre at personopplysninger blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren kan behandle opplysninger.

Det foreligger kun en databehandlerrelasjon hvis oppdraget man gir den andre virksomheten går ut på å behandle personopplysninger på vegne av sin virksomhet. For at det skal foreligge en databehandlerrelasjon er det altså en forutsetning at den andre parten faktisk behandler personopplysninger, og at formålet helt eller delvis går ut på å behandle personopplysninger. Noen eksempler på systemer som behandler våre personopplysninger, og som vi trenger databehandleravtaler med, er Visma og Elements.

Alta kommune setter i dag ut mye av sin behandling av personopplysninger til en databehandler. Ofte kan det dreie seg om lagring i skyen, men også andre typer behandlinger blir satt ut av kommunen. Reglene rundt databehandler og databehandleravtaler finnes i artikkel 28 og 29.

Ved erfaringsutvekslingsmøter med personvernombud i andre kommuner fant ombudet ut at andre kommuner opererer med egne databehandleravtaler, og at de som hovedregel legger ved sin databehandleravtale når de sender ut anbud. Alta kommune hadde også sin egen databehandleravtale, men ved møter og samtaler med innkjøpsavdelingen ble det erfart at den ikke blir brukt i praksis. Det ble raskt konstatert at leverandørene ikke ønsket å bruke Alta kommunes databehandleravtale, og de pekte særlig på punktet om mislighold. Leverandørene så på innholdet som urimelig og noe de ikke kunne signere på. Som følge av dette ble det satt i gang et arbeid om å revidere Alta kommunes databehandleravtale.

Det ble først gjennomført en rekke møter for innspill på den gamle avtalen. Innspillene ble hyppig anvendt i sammenfatningen av den nye avtalen. Når ny avtale skulle utarbeides ble det også sett hen til andre kommuners og virksomheters avtaler. Deretter ble det trukket ut momenter som ombudet fant aktuelle. Videre ble det produsert et dokument der personvernombudet kommenterte endringer fra gammel til ny avtale, de momenter som hadde blitt hentet fra andre databehandleravtaler, og hva som var ombudets egne skrevne ord. Alta kommunes databehandleravtale er nå ferdigstilt, og har vært oppe til behandling i ledergruppa. Den er formidlet til innkjøpsavdelingen, og videre arbeid blir å formidle den til resten av de ansatte som inngår avtaler, samt andre som finner det relevant å ha den.

3.4 VURDERING AV PERSONVERNKONSEKVENSER (DPIA)

Når man gjør Data Protection Impact Assessment (DPIA) så vurderer man personvernkonsekvenser. Dette er en ny plikt for virksomheter som behandler personopplysninger, og plikten er hjemlet i personvernforordningen artikkel 35. Bestemmelsen definerer når det er påkrevd å gjøre en DPIA, hva den skal inneholde, og hvem som skal gjennomføre den.

Det er den behandlingsansvarlige, altså Alta kommune, som er ansvarlig for å sikre at vurdering av personvernkonsekvenser gjennomføres. Vurderingen kan gjennomføres innenfor eller utenfor virksomheten, men det er den behandlingsansvarlige som har det øverste ansvaret for denne oppgaven. I samråd med leder er det vurdert at personvernombudet har bredest kompetanse til å kunne vurdere personvernkonsekvenser. Personvernombudet vurderer og kontrollerer derfor DPIA'ene.

Vurdering av personvernkonsekvenser er bare obligatorisk dersom behandlingen sannsynligvis vil medføre en høy risiko for fysiske personers rettigheter og friheter. Det betyr at før man gjennomfører en DPIA må man først vurdere om behandlingen vil medføre en høy risiko. Kort oppsummert trenger man først å vurdere 1) om man trenger å gjøre en full personvernkonsekvensvurdering, og hvis ja: 2) gjøre en full

personvernkonsekvensvurdering.

For å kunne gjøre disse vurderingene trenger man skjemaer å fylle inn. Alta kommune har ikke hatt skjemaer for å kunne gjennomføre personvernkonsekvensvurderinger. Dette har personvernombudet utarbeidet. Disse to typene av skjemaer er i bruk nå.

3.5 PERSONVERNBRUDD

Personvernbrudd er definert i personvernforordningen artikkel 4 nr. 12 hvor det står at:

«Et brudd på personopplysningssikkerheten, er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.»

Dette kan kategoriseres i:

- Brudd på **konfidensialitet**, det vil si at det har vært en utilsiktet eller ulovlig utlevering av, eller tilgang til, personopplysninger.
- Brudd på **integritet**, det vil si at det har vært en utilsiktet eller ulovlig endring av personopplysninger.
- Brudd på **tilgjengelighet**, det vil si der det har vært et utilsiktet eller ulovlig tap av tilgang til, eller tilintetgjøring av, personopplysninger.

Et brudd kan omfatte én, eller en kombinasjon av disse tre.

Utgangspunktet er at alle brudd på personopplysning sikkerheten skal meldes til Datatilsynet innen 72 timer, dette er regulert i artikkel 33 nr. 1. Her er en viktig presisering at det er snakk om 72 klokketimer fra virksomheten ble kjent med bruddet. Rutiner for håndtering av brudd på personopplysningssikkerheten bør derfor innarbeides i beredskapsplaner og i rutiner for håndtering av andre sikkerhetshendelser.

I noen tilfeller vil det ikke være nødvendig å melde avviket til Datatilsynet, det er i de tilfellene bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Med en gang man er klar over at det er har skjedd et brudd, skal man selvsagt håndtere og begrense det, men virksomheten må samtidig avgjøre hvilken risiko det kan ha medført for de som er berørt av bruddet.

Når man skal vurdere risiko av et brudd må man se på de konkrete omstendighetene rundt et brudd, herunder dens alvorlighetsgrad og potensielle innvirkning. For å avgjøre dette kan man se på følgende kriterier som må vurderes mot hverandre:

- Hva slags type brudd er det

- Personopplysningenes art, sensitivitet og mengde
- Hvor lett det er å identifisere enkeltpersoner
- Alvorlighetsgrad av konsekvenser for enkeltpersoner
- Spesielle egenskaper ved enkeltpersoner
- Antall berørte enkeltpersoner
- Spesielle egenskaper ved den behandlingsansvarlige

Dersom bruddet ikke vil medføre risiko for de berørte er det ikke nødvendig å melde avvikt til Datatilsynet.

En rutine for hvordan å håndtere personvernbrudd er påbegynt.

3.6 INNSYNSBEGJÆRING

Den som er registrert har rett på innsyn i hvilke personopplysninger som er lagret om seg selv, personopplysninger til eget barn under 18 år, eller en person den handler på vegne av og har fullmakt fra. Dette følger av personvernforordningen artikkel 38 nr. 4. En rutine for hvordan man går frem ved slike innsynsbegjæringer har ikke eksistert. En slik rutine er påbegynt, og skal sikre saksgang fra mottatt henvendelse til utlevering av personopplysninger til den registrerte.

Alta kommune må være sikker på at det ikke gis ut personopplysninger til andre enn den som har rett til å se disse, og sikre at de sendes ut på en sikker måte. Opplysningene som er vurdert som offentlige kan sendes per e-post. Opplysninger som er unntatt offentlighet skal sendes til folkeregistrert adresse eller sikker digital postboks. I saker med særskilt beskyttelsesbehov skal opplysningene sendes rekommandert.

Alta kommune har ikke hatt rutine for hvordan man håndterer innsynsbegjæringer, og hvordan man går fram ved en slik forespørsel. En slik rutine skal blant annet inneholde hvem man skal kontakte for å få tak i informasjon, hvilke systemer vi oppbevarer personopplysninger i, hvordan man skal svare vedkommende i en slik forespørsel, tidsbruk, hvordan dokumentene skal sendes ut, samt annen relevant informasjon. Dette rutinen er ferdigstilt.

4. PROFILERING, PUBLISERING OG TILSTEDEVÆRELSE

Å øke bevisstheten til ledere og ansatte når det gjelder personvern anses som en viktig oppgave for personvernombudet. Når folk er opplyste øker sannsynligheten for at de er med på å gjennomføre nødvendige tiltak. Å få ledere og ansatte opplyste på et område som personvern, krever tilstedeværelse.

Personvernombudet er av den oppfatning av at måten å gjøre dette på er å publisere på internett og intranett, invitere seg ut i personalmøter og delta på interne kurs, lage og bruke profileringsmateriell med farger og ikoner mm. På denne bakgrunn har ombudet designet ulike profileringsikoner, og fått kommunikasjonsrådgiver til å lage disse i photoshop. Profileringsikonene vil være et hjelpemiddel for å nå ut til flest mulig. Nedenfor fremkommer et eksempel. Her er overskriften «Webinar» brukt. De andre profileringsikonene ser like ut, men har andre overskrifter som blant annet «5 personverntips», «personvettreglene», «grunnleggende personvern» mm.

Disse ikonene er allerede brukt ved publisering på intranett, på hjemmesiden, samt på Alta kommunes Facebook-side. I 2022 vil videre publisering fortsette.

Når det gjelder fysisk tilstedeværelse har personvernombudet hittil fått muligheten til å delta med materiale på utvidet ledermøte, ledermøter, personalmøter ol. Videre har

ombudet blitt kontaktet av både virksomhetsledere, avdelingsledere, styrere osv. fordi de ønsker rådgivende informasjon fra personvernombudet. Særlig er det ulike typer caser de opplever i sin arbeidshverdag de ønske drøfte. Disse møtene kommer på løpende bånd i 2022, og ombudet finner det høyst fantastisk at lederne tar kontakt for avklaringer, møter og kurs. Dette viser tydelig at lederne ønsker å lære om personvern, og at de ønsker å ha kontroll og orden.

5. INTERNKONTROLL, INFORMASJONSSIKKERHET OG PERSONVERN

5.1 DEFINISJONER OG SAMMENHENGEN

Internkontroll er en prosess, gjennomført av styrer, ledelser og ansatte, som er utformet for å gi rimelig sikkerhet for måloppnåelse på følgende områder: målrettet og effektiv drift, pålitelig rapportering, og overholdelse av lover og regler. Internkontrollforskriften inneholder 8 opplistede krav til internkontrollen. Disse kravene kan anses som en smørbrødliste:

1) Skaffe oversikt over lover og forskrifter som gjelder for din bedrift.
2) Sørge for at ansatte har tilstrekkelig kunnskap og ferdigheter i HMS.
3) Sørge for at ansatte medvirker.
4) Fastsette mål for HMS.
5) Organisasjonskart og ansvarsområder.
6) Kartlegging og risikovurdering.
7) Etablere rutiner for avvik.
8) Revisjon av internkontrollen.

Internkontroll er leders redskap for å styre risiko på informasjonssikkerhetsområdet. Internkontroll er bedriftens egenkontroll. Det er en kvalitetssikring på at bedriften har systemer og rutiner som fungerer, og som fanger opp problemer og utfordringer i tide.

Informasjonssikkerhet er et tema hvor det anvendes ulike begreper ut i fra ulike fagområder. Begrepsbruken kan også variere ut i fra ulike regelverk. På denne bakgrunn er det derfor viktig å avklare innholdet i begrepene man bruker når man er i dialog med andre. Informasjonssikkerhet, digital sikkerhet, cybersikkerhet og IKT-sikkerhet er ulike begreper som ofte benyttes synonymt med hverandre. Innholdet i disse eksemplene anses som det samme sett fra forskjellige perspektiver.

Informasjonssikkerhet dreier seg om å håndtere risikoen for at personopplysninger og andre informasjonsverdier blir ivaretatt på en tilfredsstillende måte. Dette gjøres ved først å identifisere hvilke personopplysninger virksomheten har. Deretter gjennomføres en risikovurdering for å avklare om eksisterende sikkerhetstiltak er tilfredsstillende.

Dersom risikovurderingen avdekker manglende tiltak må det vurderes om nye tiltak skal iverksettes for å oppnå tilfredsstillende sikkerhetsnivå for personopplysningene. Kontrollrutiner må utarbeides og jevnlig følges, for å kontrollere at tiltakene blir fulgt opp og virker etter hensikten.

En slik fremgangsmåte som skissert ovenfor vil sammen med tilhørende rutiner kunne utgjøre virksomhetens styringssystem for informasjonssikkerhet. Dette systemet for informasjonssikkerhet vil være en sentral del av virksomhetens internkontroll. Det er utviklet standarder som beskriver hvordan styringssystem for informasjonssikkerhet skal etableres.

Det er vanlig å si at det handler om å sikre at informasjon i alle former:

1) Ikke blir kjent for uvedkommende (konfidensialitet)
2) Ikke blir endret utilsiktet eller av uvedkommende (integritet)
3) Er tilgjengelig ved behov (tilgjengelighet)

Informasjonssikkerhet er knyttet til blant annet personvernbrudd, og handler om å klare å håndtere risikoen knyttet til dette.

Personvernregelverket krever at personopplysninger skal beskyttes tilfredsstillende mot uberettiget innsyn og endringer. Samtidig skal opplysningene være tilgjengelige for de som trenger opplysningene, når de har behov for dem.

Gjennom å ha god internkontroll og god informasjonssikkerhet sikrer virksomheten at den behandler personopplysninger lovlig, sikkert og forsvarlig.

5.2 TRUSLER MOT INFORMASJONSSIKKERHETEN; DATAANGREP

PST vurderer dataangrep, sammen med høyreekstremisme og ekstrem islamistisk overbevisning, som de største truslene mot stat og kommune i 2022. Høsten 2020 ble Stortinget utsatt for dataangrep. På grunnlag av dette varsler Datatilsynet nå et overtredelsesgebyr på 2 millioner kroner.

Bakgrunnen for gebyret er at Stortingets administrasjon ikke skal ha gjennomført egnede tekniske og organisatoriske tiltak for å oppnå et tilstrekkelig sikkerhetsnivå. Det er særlig lagt vekt på at Stortinget ikke hadde etablert tofaktorautentisering eller tilsvarende effektive sikkerhetstiltak for å oppnå tilstrekkelig beskyttelse. Dataangrepet var nemlig knyttet til uautorisert pålogging til e-postkontoene til et ukjent antall stortingsrepresentanter og ansatte i administrasjonen og gruppesekretariatene.

I januar 2021 ble Østre Toten kommune utsatt for et alvorlig cyberangrep. Som konsekvens fikk ansatte ikke lenger tilgang til de fleste av kommunens IT-systemer, kommunens data var blitt kryptert og sikkerhetskopier slettet. Løsepengebrev ble funnet på en mengde lokasjoner. I mars 2021 ble det kjent at deler av dataene hadde blitt publisert på det mørke nettet («dark web»). Kommunen har anslått at ca. 30 000 dokumenter var omfattet av angrepet. Dokumentene inneholdt dels svært sensitive

opplysninger om kommunens innbyggere og ansatte. Datatilsynet vurderte at det var store og grunnleggende mangler ved Østre Totens personopplysningssikkerhet. På grunnlag av dette ble Østre Toten kommune ilagt et overtredelsesgebyr på 4 millioner kroner. Kommunen ble også pålagt å implementere et egnet styringssystem for informasjonssikkerhet og personopplysningssikkerhet. Ordføreren mente de hadde tapt anslagsvis 35 millioner kroner. 1000 datamaskiner måte gjenopprettes, og 1300 ansatte jobbet i lang tid med penn og papir.

I juni 2021 ble Tromsø kommune utsatt for dataangrep. 15 000 e-poster med spam ble forsøkt sendt ut fra kontoen til en ansatt. Tromsø kommune har uttalt at de ikke kan utelukke at sensitiv informasjon har kommet på avveie. IT-sjefen mente at det kunne være flere grunner til at den ansattes e-post ble hacket; Skadevare på maskinen, at den ansatte har eksponert passordet sitt til noen andre, eller at den ansatte har trykket på en tilsendt link.

Tromsø kommune hadde tilgang til sikkerhetssystem med totrinnsverifisering, som vil si at man må logge seg på en konto i to trinn og ofte ved hjelp av en telefon. En slik metode gjør det vanskeligere for uønskede å få tilgang til kontoer. I Tromsø kommune ble slike metoder kun brukt der det var pålagt, og følgen av dette var at mange ansatte ikke brukte sikkerhetssystemet selv om det var mulig å bruke det.

Dataangrepet mot blant annet Stortinget, Østre Toten kommune og Tromsø kommune er tre eksempler på de mange tusentalls dataangrep Norge har vært utsatt for. Disse angrepene er i tillegg bare begynnelsen på det vi kan forvente. Med en økende digitalisering blir hackere flinkere, og det utvikles stadig nye metoder for å nå fram til sensitiv informasjon. Eksperter ser blant annet en økende bruk av det som kalles botnett. Et *botnett* er et nettverk av datamaskiner infisert av datavirus eller trojanske hester. Disse maskinene kobler seg til en eller flere sentrale styrende noder der de får tildelt oppgaver. Oppgavene kan være å søke gjennom nettsider etter e-postadresser, sende ut uønsket søppelpost (spam) eller å utføre tjenestenektangrep mot utvalgte mål på internett. Et botnett kan bestå av tusentalls datamaskiner, ofte kalt zombier, spredd over hele verden og med eiere som ikke vet at maskinene er infiserte.

Dataangrep forårsaker store skader, og er en stor økonomisk belastning for en angrepet stat eller kommune. En økonomisk belastning er at man risikerer bøter og gebyrer fra Datatilsynet dersom man ikke har hatt gode nok sikkerhetssystemer. En annen økonomisk belastning blir den ressursbruken som anvendes etter selve angrepet.

Å sikre seg helt mot dataangrep er så å si en umulig oppgave, men det finnes tiltak man kan gjøre for å minke sannsynligheten. Å unngå å klikke på vedlegg eller linker fra ukjente avsendere eller fra mistenkelige e-poster er et sikkert tiltak. Særlig er svindelmetoden *phishing* utbredt. Phishere prøver å utgi seg for å være kjente organisasjoner, for eksempel banker eller høyt profilerte forhandlere, i et forsøk på å skaffe brukerinformasjonen din, eller å levere skadelig programvare til enheten din via mistenkelige lenker eller vedlegg i e-postmeldinger. Dersom man skulle være

uheldig å bli utsatt for et slikt type angrep, er det viktig at de ansatte i forkant er bevisste på å bytte passord ofte, og at man lager sterke passord med tall, store bokstaver og spesialtegn. Videre er det viktig å operere med ulike passord på ulike plattformer. Ved å bruke ulike passord er risikoen lavere for at uvedkommende får tilgang til andre plattformer også.

Den stadig økende andelen av skyløsninger aktualiserer behovet for å kunne stadfeste identiteten til de ansatte på en bedre måte. Tidligere baserte man seg på at man kun kunne få tilgang til kommunens systemer dersom man var fysisk plassert i kommunens nettverk. Nå er man i større grad avhengig av autentisering med flere faktorer, for eksempel både passord og kode på mobil. Det jobbes også med løsninger hvor eksempelvis fingeravtrykk og ansiktsgjenkjenning kan brukes som en ekstra faktor.

Et viktig tiltak mot cyberangrep er å ha gode styrings- og sikkerhetssystemer. Tildelingskriterier, sertifikater, kryptering og brannmurer er eksempler som inngår i sikkerhetssystemer.

Alta kommune har på plass gode tiltak for å sikre seg mot vanlige trusler som svindelepost, virus og vilkårlige angrep fra internett. Målrettede angrep fra kriminelle og statlige aktører er vanskeligere å forsvare seg mot. Muligheten for å oppdage slike angrep når de først har skjedd er mangelfull. Løsninger som beskytter bedre mot slike trusler må vurderes. De er imidlertid kostbare og må vurderes opp mot risikoen man løper ved å ikke ha slike løsninger.

Ved en oppsummering vil de viktigste oppgavene på dette området bli 1) å øke bevisstheten blant ledere og ansatte, i tillegg til 2) å styrke styrings- og sikkerhetssystemene for Alta kommune.