# Innhold

1. Innledning og formål ..... 3
2. Ansvar ..... 3
3. Internkontroll ..... 4
3.1 Beskrivelse av kontrollrutiner ..... 4
3.2 Cyberbooks sikkerhetsmål ..... 4
4. Behandling av personopplysninger i Cyberbook ..... 5
4.1 Oversikt over behandling av personopplysninger ..... 5
4.2 Risikobasert tilnærming ..... 5
4.3 Vurdering av personvernkonsekvenser (DPIA) ..... 6
4.4 Oppfølgning av tiltak fra risikovurdering ..... 6
4.5 Rutine for endringshåndtering ..... 6
4.6 De ansattes epost og personlige filer ..... 7
4.6.1 Lagring av kunderelaterte dokumenter i Cyberbooks kundehåndteringssystem ..... 7
4.6.2 De ansattes bruk av elektronisk utstyr mv. ..... 7
4.6.3 Cyberbooks innsyn i ansattes epost m.v. ..... 7
4.6.4 Avslutning av epostkasse og sletting ved opphør av arbeidsforholdet ..... 8
5. Databehandling av andre på vegne av Cyberbook ..... 8
5.1 Oversikt over databehandlere ..... 8
5.2 Plikt til å inngå databehandleravtaler ..... 8
5.3 Taushetserklæring ..... 9
5.4 Overføring av personopplysninger til tredjeland ..... 9
6. Cyberbooks behandling av personopplysninger på vegne av behandlingsansvarlige (kunder) ..... 9
7. Sikkerhetstiltak ..... 9
7.1 Organisatoriske tiltak ..... 10
7.1.1 Intern organisering ..... 10
7.1.2 Taushetsplikt for personale (ledelse, ansatte og oppdragstakere) ..... 10
7.2 Tekniske tiltak ..... 10
7.2.1 Tilgangskontroll for IT-systemer ..... 10
7.2.2 IT-sikkerhet ..... 10
7.3 Fysiske tiltak ..... 10

8. Avvik og varsling ..... 11
8.1 Varsling til Datatilsynet når Cyberbook er behandlingsansvarlig ..... 11
8.2 Varsling til de registrerte når Cyberbook er behandlingsansvarlig ..... 11
8.3 Varsling til den behandlingsansvarlige når Cyberbook er databehandler ..... 12
9. Rutiner for ivaretakelse av de registrertes rettigheter ..... 12
9.1 Mottak av henvendelser ..... 12
9.2 Anmodning om innsyn ..... 12
9.3 Anmodning om retting ..... 13
9.4 Anmodning om sletting ..... 14
9.5 Rett til begrensning av behandlingen ..... 14
9.6 Rett til å protestere mot behandlingen ..... 15
9.7 Dataportabilitet ..... 15

# 1. Innledning og formål

Disse rutinene for informasjonssikkerhet og behandling av personopplysninger er vedtatt av daglig leder i Cyberbook. De gjelder all behandling av personopplysninger i Cyberbook.

I henhold til personopplysningsloven og EU personvernforordning (GDPR) skal det gjennomføres egnede tekniske og organisatoriske tiltak for å sikre og dokumentere at personopplysninger behandles i samsvar med loven. Disse rutinene skal sikre at tilstrekkelige tiltak er iverksatt og følges opp ved selskapets behandling av personopplysninger.

Rutinene skal blant annet legge til rette for at ved systematiske tiltak ivaretar integriteten, konfidensialiteten og tilgjengeligheten til personopplysninger som Cyberbook til enhver tid oppbevarer eller behandler på annen måte, samt robustheten til Cyberbook som organisasjon og systemene Cyberbook benytter til behandling av personopplysninger.

I disse rutinene menes med:

«*konfidensialitet*» – at informasjonen ikke blir kjent for uvedkommende,

«*integritet*» – at informasjonen ikke blir endret utilsiktet eller av uvedkommende,

«*tilgjengelighet*» – at informasjonen er tilgjengelig for autoriserte ved behov, og

«*robusthet*» – at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser.

# 2. Ansvar

Cyberbooks ledelse har det overordnede ansvaret for at Cyberbook behandler personopplysninger i henhold til den til enhver tid gjeldende lovgivning. Ledelsen har herunder ansvar for at det faktisk gjennomføres egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med det til enhver tid gjeldende regelverk. Dette inkluderer ansvaret for å forvalte, vedlikeholde og følge opp etterlevelsen av disse rutinene, og å påse at det er etablert systemer og prosedyrer for oppfølging av rutinene og at roller, ansvarsforhold og rapporteringsveier er definert og kjent.

Enhver som er ansatt eller på annet grunnlag er involvert i Cyberbooks behandling av personopplysninger, har et individuelt ansvar, og plikter å bidra til at personopplysninger behandles etter disse rutinene og etter det til enhver tid gjeldende regelverk for behandling av personopplysninger.

Hvis det er usikkerhet om hvordan personopplysninger skal behandles, skal behandlingen avventes til dette er avklart av ledelsen, eventuelt etter konsultasjon med Datatilsynet eller eksterne rådgivere.

# 3. Internkontroll

## 3.1 Beskrivelse av kontrollrutiner

Cyberbooks ledelse skal gjennomføre årlige gjennomganger av rutinene for å sikre:

- At behandlingsoversikten (vedlagt) omfatter all behandling av personopplysninger som Cyberbook utfører (på egne eller kunders vegne)
- At sikkerhetsmålene angitt i punkt 3.2 oppnås
- At det gjøres korrigerende tiltak ved avvik
- At det sørges for at Cyberbooks internkontroll og styringssystem for informasjonssikkerhet er hensiktsmessige, tilstrekkelig og effektive
- At Cyberbook oppfyller gjeldende personvernlovgivning

Daglig leder eller den daglig leder utpeker skal sørge for å innkalle og organisere gjennomgangen. Gjennomgangen skal dokumenteres. I referatet fra gjennomgangen skal det være klart angitt hvilke tiltak som er besluttet og med hvilken begrunnelse.

Gjennomgangen skal baseres på følgende bakgrunnsmateriale:

- Resultater og hovedkonklusjoner fra risikoanalyser og egenkontroll
- Endringer i personvernreglene eller offentlige sikkerhetskrav
- Vurderinger om tilstrekkelige ressurser er tilgjengelige for å ivareta internkontroll og informasjonssikkerhet

## 3.2 Cyberbooks sikkerhetsmål

Sikkerhetsmålene beskriver Cyberbooks overordnete mål for beskyttelse av de personopplysningene Cyberbook behandler på egne vegne (som behandlingsansvarlig) og på vegne av sine kunder (som databehandler). Cyberbook har vedtatt følgende sikkerhetsmål:

1) Cyberbook skal sikre at personopplysninger behandles i henhold til gjeldende lovgivning på området.
2) Cyberbook skal hindre at uvedkommende får adgang til lokaler der personopplysninger og andre opplysninger kan være lagret og behandles.
3) Tilgang til Cyberbooks systemer og informasjon gis kun til medarbeidere etter behov («need to know») og tilgang til systemer og informasjon for uvedkommende skal forhindres.
4) Cyberbook skal sikre at behandlingen av personopplysninger er korrekt og at opplysninger ikke endres uten lovlig grunnlag.
5) Det skal foreligge rutiner for å håndtere uønskede hendelser, og det skal være mulig å spore slike uønskede hendelser.
6) Det skal forhindres at personer eller systemer hos Cyberbook bevisst eller ubevisst er årsak til uønskede hendelser mot egen virksomhet eller personvernet til fysiske personer.
7) Cyberbook skal sikre at medarbeidere og andre som bruker Cyberbooks informasjonssystemer og behandler personopplysninger har tilstrekkelig kompetanse til å ivareta Cyberbooks og kundenes sikkerhetsbehov/ -krav.

# 4. Behandling av personopplysninger i Cyberbook

## 4.1 Oversikt over behandling av personopplysninger

Cyberbook behandler personopplysninger for å administrere forholdet til sine ansatte og innleide konsulenter, kunder og leverandører.

Cyberbook fører en oversikt over behandling av personopplysninger i Cyberbook («Behandlingsoversikten»).

Behandlingsoversikten inneholder:

- Hvilke informasjonssystemer som benyttes for å behandle personopplysninger
- Hvem det behandles personopplysninger om
- Hvilke kategorier av personopplysninger som behandles
- Om det behandles særlige kategorier av personopplysninger ("sensitive personopplysninger"), og eventuelt behandlingsgrunnlag for behandling av slike opplysninger.
- Formålet med behandlingen
- Det rettslige grunnlaget for behandlingen (behandlingsgrunnlaget)
- Rutiner for sletting
- Hvem som er behandlingsansvarlig
- Hvem opplysningene deles med
- Om det er gjennomført risikovurdering
- Beskrivelse av tekniske eller organisatoriske tiltak for å sikre behandlingen ut over de generelle sikkerhetstiltakene som følger av disse rutinene for informasjonssikkerhet og behandling av personopplysninger
- Rutiner og ansvarsplassering for ivaretakelse av de registrertes rettigheter
- Hvilken informasjon som gis den registrerte om behandlingen
- Om det benyttes databehandler og om det er inngått databehandleravtale
- Om det skjer overføring av personopplysninger til utenfor EØS, og eventuelt grunnlag for slik overføring

Alle områder i Cyberbook skal være dekket av Behandlingsoversikten. Oversikten skal gjennomgås årlig for å vurdere om den er dekkende.

Den til enhver tid gjeldende Behandlingsoversikten inngår som del av disse rutinene og skal alltid følge som vedlegg til rutinene (vedlegg A).

## 4.2 Risikobasert tilnærming

Cyberbooks arbeid med informasjonssikkerhet og behandling av personopplysninger skal være risikobasert. Med risiko menes her en funksjon av konsekvens og sannsynlighet.

Risikoen forbundet med et system eller en forretningsprosess skal identifiseres konkret for det aktuelle systemet eller den aktuelle prosessen gjennom en risiko- og sårbarhetsanalyse («ROS»-analyse). ROS-analyser skal gjennomføres årlig og ved endringer (tekniske, regulatoriske og organisatoriske) som kan påvirke informasjonssikkerheten ved systemet eller prosessen. Hvis resultatet av ROS-analysen tilsier det, skal det gjennomføres en vurdering av personvernkonsekvenser (DPIA). Se punkt 4.3 nedenfor.

Resultatet av hver ROS-analyse skal lagres trygt, slik at det ved behov er tilgjengelig for autorisert personell.

## 4.3 Vurdering av personvernkonsekvenser (DPIA)

Hvis det er trolig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil kunne medføre en høy risiko for de registrertes rettigheter og friheter, skal det - før behandlingen tar til - foretas en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet (DPIA), og om disse konsekvensene kan fjernes eller reduseres gjennom risikoreduserende tiltak. Cyberbook skal alltid gjennomføre en vurdering av personvernkonsekvenser (DPIA) i de tilfeller som følger av Datatilsynets til enhver tid gjeldende liste over typer av behandlingsaktiviteter som innebærer krav om DPIA.

Daglig leder skal beslutte om det skal foretas vurdering av personvernkonsekvenser (DPIA).

## 4.4 Oppfølgning av tiltak fra risikovurdering

Dersom Cyberbook gjennom en ROS-analyse og/eller en vurdering av personvernkonsekvenser (DPIA) har identifisert forhold forbundet med et system eller forretningsprosess som innebærer risiko for brudd på personopplysningssikkerheten, skal Cyberbook samtidig identifisere tekniske og/eller organisatoriske tiltak som kan gjennomføres og som vil fjerne eller redusere denne risikoen.

Der den identifiserte risikoen er høy, dvs. dersom konsekvensen av bruddet vil være alvorlig og sannsynligheten for at det vil oppstå brudd er høy, skal Cyberbook alltid enten gjennomføre risikoreduserende tiltak eller unnlate å foreta den behandling som utløser den identifiserte risiko. Der den identifiserte risikoen er middels eller lav, fordi konsekvensen av bruddet vil være lav og/eller det er liten sannsynlighet for at bruddet vil oppstå, kan Cyberbook etter en konkret vurdering av risiko sett opp mot kostnadene ved risikoreduserende tiltak eller konsekvensen av unnlatt behandling beslutte å akseptere risikoen eller å kun gjennomføre mindre omfattende tiltak.

Cyberbook skal treffe beslutning om å gjennomføre risikoreduserende tiltak så snart dette er praktisk mulig etter at tiltakene er identifisert. Beslutningen skal dokumenteres skriftlig.

Daglig leder har ansvaret for å vurdere om og evt. hvilke risikoreduserende tiltak som skal gjennomføres, og for å sørge for at tiltakene blir gjennomført.

## 4.5 Rutine for endringshåndtering

Dersom Cyberbook vurderer å endre sine informasjonssystemer eller gjennomføre andre endringer i sin behandling av personopplysninger (jf. behandlingsoversikt beskrevet i pkt. 4.1 over), skal

Cyberbook samtidig gjennomføre en ROS-analyse etter punkt 4.2 og eventuelt en vurdering av personvernkonsekvenser etter pkt. 4.3. I vurderingen av om endringen skal gjennomføres, skal Cyberbook legge vekt på om den endrede behandlingen innebærer økt risiko for brudd på personopplysningssikkerheten, og om denne risikoen kan fjernes eller reduseres ved risikoreduserende tiltak i henhold til pkt. 4.4. Vurderingen skal dokumenteres skriftlig.

Cyberbook skal ikke gjennomføre endringer som vil innebære høy risiko for brudd på personopplysningssikkerheten som ikke kan fjernes eller reduseres ved risikoreduserende tiltak. Cyberbook kan likevel gjennomføre slike endringer dersom Cyberbook har gjennomført forhåndsdrøftinger med Datatilsynet etter GDPR Artikkel 36.

Behandlingsoversikten (jf. pkt. 4.1) skal oppdateres slik at den gjenspeiler foretatte endringer.

## 4.6 De ansattes epost og personlige filer

### 4.6.1 Lagring av kunderelaterte dokumenter i Cyberbooks kundehåndteringssystem

Når en ansatt via epost eller på annen måte mottar dokumenter som gjelder Cyberbooks kunder, så som kontrakter, bestillinger og opplysninger om kundens kontaktpersoner, skal den ansatte uten opphold sørge for å lagre dokumentene på kundens side i Cyberbooks kundehåndteringssystem. Den ansatte kan ikke bruke sin egen epostkasse eller personlige filområde til permanent lagring av slike dokumenter.

En ansatt som avslutter sitt ansettelsesforhold hos Cyberbook skal forut for fratredelse gå gjennom sin epost og personlige filområde og forsikre seg om at alle kunderelaterte dokumenter som den ansatte har mottatt er lagret på riktig måte i Cyberbooks kundehåndteringssystem.

### 4.6.2 De ansattes bruk av elektronisk utstyr mv.

Cyberbook stiller elektroniske tjenester og elektronisk utstyr til rådighet for de ansatte til bruk i arbeidet. De ansatte kan bare bruke slike elektroniske tjenester og utstyr til å utføre sine arbeidsoppgaver for Cyberbook. Den ansatte kan likevel benytte slikt utstyr til private formål, forutsatt at dette kan skje uten at bruken forhindrer eller vanskeliggjør utførelsen av arbeidsoppgavene, eller at bruken innebærer fare for datasikkerheten i Cyberbook. Den ansatte kan således ikke bruke Cyberbooks tjenester eller utstyr på en måte som innebærer risiko for datavirus eller andre former for sikkerhetsbrudd, eller til bruk som innebærer brudd på loven (så som ulovlig deling av opphavsrettsbeskyttet materiale). Den ansatte skal dessuten bidra til å overholde Cyberbooks datasikkerhetstiltak slik disse er til enhver tid (jf. pkt. 7 nedenfor).

Cyberbook har rett til å overvåke den ansattes bruk av elektronisk utstyr, herunder bruk av internett, når formålet med overvåkningen er å administrere Cyberbooks datanettverk eller å avdekke eller oppklare sikkerhetsbrudd i nettverket. Cyberbook kan ikke overvåke den ansattes bruk for andre formål.

### 4.6.3 Cyberbooks innsyn i ansattes epost m.v.

Cyberbook har kun rett til innsyn i den ansattes e-postkasse eller filer lagret på den ansattes personlige filområde dersom dette er nødvendig for å ivareta den daglige driften eller andre berettigede interesser ved virksomheten, eller ved begrunnet mistanke om at den ansattes bruk av

e-postkassen eller annet elektronisk utstyr medfører grovt brudd på de de plikter som følger av arbeidsforholdet eller kan gi grunnlag for oppsigelse eller avskjed.

Cyberbook skal så langt mulig varsle den ansatte og gi den ansatte anledning til å uttale seg, før Cyberbook gjennomfører innsyn. I varselet skal Cyberbook begrunne hvorfor vilkårene for innsyn anses å være oppfylt og orientere om den ansattes rettigheter i forbindelse med innsynet.

Den ansatte har rett til å komme med innsigelser mot innsynet, og skal så langt mulig gis anledning til å være til stede under gjennomføringen av innsynet og har rett til å la seg bistå av tillitsvalgt eller annen representant.

Dersom Cyberbook har foretatt innsyn uten forutgående varsel eller uten at den ansatte var til stede, skal Cyberbook gi den ansatte skriftlig underretning om dette så snart innsynet er gjennomført. Underretningen skal begrunne hvorfor vilkårene for innsyn var oppfylt og inneholde opplysninger om hvilken metode for innsyn som ble benyttet, hvilke e-poster eller andre dokumenter som ble åpnet samt resultatet av innsynet.

#### 4.6.4 Avslutning av epostkasse og sletting ved opphør av arbeidsforholdet

Når en ansatt slutter, skal den ansattes e-postkasse normalt avsluttes samtidig med at den ansatte fratrer. Cyberbook kan likevel holde e-postkontoen åpen i en kort periode etter fratredelse dersom det foreligger særskilt behov for dette, f.eks. knyttet til ivaretakelse av kundeforhold. I et slikt tilfelle skal Cyberbook senest med virkning fra fratredelsesdato aktivere «autosvar»-funksjonen med en melding om at den ansatte har sluttet, samt om hvordan avsender kan få kontakt med Cyberbook. Cyberbook kan for øvrig ikke foreta innsyn i e-postkassen, annet enn i de tilfeller som er beskrevet i pkt. 4.6.3 over.

E-post i e-postkassen og den ansattes personlige filer som ikke er nødvendig for den daglige driften av Cyberbook skal slettes innen rimelig tid etter at den ansatte fratrer.

# 5. Databehandling av andre på vegne av Cyberbook

## 5.1 Oversikt over databehandlere

Fysiske eller juridiske personer som behandler personopplysninger på vegne av Cyberbook, er Cyberbooks databehandlere. Oversikt over alle databehandlere skal fremgå av Behandlingsoversikten.

## 5.2 Plikt til å inngå databehandleravtaler

Det skal alltid inngås avtale med databehandlere. Avtalen skal regulere hvordan databehandleren skal håndtere og sikre personopplysningene databehandleren behandler på vegne av Cyberbook. Det skal sikres at databehandlere skal behandle opplysninger bare etter instruks fra Cyberbook.

Ledelsen er ansvarlig for at det foreligger databehandleravtaler med relevante databehandlere.

### 5.3 Taushetserklæring

Ansatte og innleide konsulenter som har tilgang til personopplysninger, herunder til system hvor det behandles personopplysninger, skal ha avgitt taushetserklæring.

### 5.4 Overføring av personopplysninger til tredjeland

Dersom personopplysninger skal overføres til tredjeland, dvs. land utenfor EU/EØS, skal det foreligge et lovlig grunnlag for overføringen etter personvernregelverket. Overføringen skal også være godkjent av Cyberbooks ledelse.

Cyberbook skal søke å begrense overføring av personopplysninger til tredjeland, og det skal ikke benyttes databehandler eller tjenester i tredjeland dersom det foreligger like bra alternativer innenfor EU/EØS eller om behandlingen kan skje på en måte som gjør at det ikke er nødvendig med overføring til tredjeland.

## 6. Cyberbooks behandling av personopplysninger på vegne av behandlingsansvarlige (kunder)

I tilfeller hvor Cyberbook behandler personopplysninger på vegne av en kunde, er Cyberbook kundens databehandler. Kunden er i slike tilfeller behandlingsansvarlig og bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.

Når Cyberbook er databehandler, skal det alltid inngås en databehandleravtale med den behandlingsansvarlige. Cyberbook skal ikke behandle personopplysninger ut over eller på annen måte enn det som følger av databehandleravtalen, instruks fra den behandlingsansvarlige eller personvernregelverket.

Cyberbook skal påse at bare autorisert personell som har avgitt taushetserklæring (eller er underlagt lovbestemt taushetsplikt), får tilgang til personopplysninger som behandles på vegne av den behandlingsansvarlige (kunden).

Ved bruk av underdatabehandlere gjelder punkt 5 tilsvarende.

## 7. Sikkerhetstiltak

Sikkerhetsmålene som følger av punkt 3.2, er styrende for Cyberbooks sikkerhetstiltak. Sikkerhetsmålene beskriver hva som ønskes oppnådd sikkerhetsmessig. Punktene nedenfor beskriver hvilke tiltak som skal gjennomføres for å oppnå sikkerhetsmålene.

## 7.1 Organisatoriske tiltak

### 7.1.1 Intern organisering

Cyberbooks ledelse er ansvarlig for at Cyberbook har de nødvendige rutiner for å gjøre behandlingen av personopplysninger forsvarlig. Ledelsen har fremdeles ansvaret selv om ansvaret er delegert og andre utfører de enkelte oppgavene.

Det skal utføres egenkontroll av sikkerhetsnivå i henhold til punkt 3 ovenfor.

Alle ansatte og innleide konsulenter skal være kjent med og følge Cyberbooks retningslinjer for passord til systemene. Ved førstegangs pålogging (til et nytt system eller som ny bruker av et eksisterende system) skal eventuelt standardpassord byttes til et personlig passord.

### 7.1.2 Taushetsplikt for personale (ledelse, ansatte og oppdragstakere)

Alle som får tilgang til personopplysninger som behandles av Cyberbook, skal avgi taushetserklæring. Taushetserklæringen kan være separat eller inngå som del av arbeids- eller oppdragsavtale.

Taushetserklæringens innhold skal besluttes av ledelsen.

## 7.2 Tekniske tiltak

### 7.2.1 Tilgangskontroll for IT-systemer

Daglig leder har ansvaret for at bare de som skal ha tilgang, er gitt tilgang til informasjonssystemene. Det skal bare gis tilganger på personnivå, ikke til brukere som deles av flere personer.

Daglig leder har ansvar for at det foreligger skriftlige rutiner for kontroll av tilgang til IT-systemene, og at kontroll gjennomføres to ganger i året.

### 7.2.2 IT-sikkerhet

Det skal til enhver tid foreligge oppdatert og gyldig sikkerhetsdokumentasjon for utstyr, programvare og systemkonfigurasjon. Daglig leder er ansvarlig for at slik dokumentasjon vedlikeholdes. Når Cyberbook benytter en databehandler, kan dette gjøres av databehandler.

Ved systemendringer og andre endringer av behandlingen av personopplysninger skal det alltid vurderes om endringene kan ha konsekvenser for informasjonssikkerheten. Dette gjelder uavhengig av om endringen beror på en lov- eller forskriftsendring, endring av en kontrakt, øvrige tekniske endringer eller organisasjonsmessige endringer.

Endringer som kan ha konsekvenser for informasjonssikkerheten, skal godkjennes av daglig leder. Ved endringer som kan ha sikkerhetsmessige konsekvenser, skal det utarbeides en risikovurdering, med forslag til tiltak, som grunnlag for beslutning av endring.

## 7.3 Fysiske tiltak

Det skal være etablert adgangskontrollsystemer med krav til adgangskort.

Det skal være vakthold som foretar rutinemessige kontroller av om uautoriserte personer befinner seg i bygget.

Ansatte som tar med seg Cyberbooks datautstyr ut av kontoret, herunder når ansatte benytter slikt utstyr på hjemmekontor eller logger seg på Cyberbooks IT-systemer via fjernpålogging, må iverksette rimelige fysiske sikkerhetstiltak som sikrer at utstyret og systemene ikke er tilgjengelig for uvedkommende. Dersom det skjer sikkerhetsbrudd, f.eks. dersom den ansatte mister eller blir frastjålet datautstyr, plikter den ansatte å varsle Cyberbook om dette så raskt som mulig.

# 8. Avvik og varsling

Ansatte som oppdager avvik fra disse rutinene eller øvrige hendelser som påvirker informasjonssikkerheten i Cyberbook, skal varsle om dette i overenstemmelse med rutinene for intern varsling i Cyberbook.

Daglig leder skal sørge for beslutning om og oppfølging av korrigerende/ forebyggende tiltak.

Ved brudd på personopplysningssikkerheten i tilfeller hvor Cyberbook er behandlingsansvarlig, har daglig leder eller den daglig leder utpeker ansvar for å varsle Datatilsynet uten ugrunnet opphold og, hvis det er mulig, innen 72 timer, samt eventuelt varsle de registrerte uten ugrunnet opphold.

Ved brudd på personopplysningssikkerheten i tilfeller hvor Cyberbook er databehandler, er daglig leder eller den daglig leder utpeker ansvarlig for å varsle den behandlingsansvarlige uten ugrunnet opphold.

## 8.1 Varsling til Datatilsynet når Cyberbook er behandlingsansvarlig

Ved brudd på informasjonssikkerheten skal Datatilsynet varsles, med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter. Cyberbook må varsle Datatilsynet selv om sikkerhetsbruddet ikke har ført til en faktisk utlevering av opplysningene.

Datatilsynet skal varsles uten ugrunnet opphold og senest innen 72 timer etter at bedriften har fått kjennskap til sikkerhetsbruddet. Dersom Cyberbook ikke er i stand til å overholde fristen på 72 timer, skal årsakene til forsinkelsen oppgis.

Cyberbook kan varsle Datatilsynet gjennom varslingsskjema tilgjengelig her:
https://www.altinn.no/skjemaoversikt/datatilsynet/melding-om-avvik-datatilsynet/

## 8.2 Varsling til de registrerte når Cyberbook er behandlingsansvarlig

Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal de registrerte varsles uten ugrunnet opphold. Datatilsynet skal også varsles i henhold til punkt 8.1 ovenfor.

Cyberbook trenger likevel ikke å varsle den registrerte direkte hvis:

1) Cyberbook har gjennomført egnede tekniske og organisatoriske sikkerhetstiltak og anvendt disse på personopplysningene som er rammet av bruddet. Dette gjelder særlig tiltak som gjør opplysningene uleselige for uautoriserte, f.eks. kryptering,

2) Cyberbook har truffet etterfølgende tiltak som sikrer at det ikke lenger er sannsynlig at den høye risikoen for de registrertes rettigheter og friheter vil oppstå, eller

3) varsling til den registrerte krever uforholdsmessig stor innsats fra Cyberbook. I så fall skal Cyberbook underrette allmennheten eller treffe lignende tiltak som sikrer at de registrerte underrettes på en like effektiv måte.

### 8.3 Varsling til den behandlingsansvarlige når Cyberbook er databehandler

Hvis Cyberbook, som databehandler, blir kjent med et brudd på personopplysningssikkerheten skal den behandlingsansvarlige varsles om dette uten ugrunnet opphold. Den behandlingsansvarlige har selv ansvar for å varsle Datatilsynet og de registrerte.

Cyberbook skal i rimelig grad bistå den behandlingsansvarlige med å bringe på det rene og dokumentere hva bruddet går ut på, hva som har forårsaket det, og hvilke konsekvenser det kan ha fått for de registrerte.

## 9. Rutiner for ivaretakelse av de registrertes rettigheter

### 9.1 Mottak av henvendelser

I tilfeller hvor Cyberbook er databehandler, skal henvendelser som vedrører de registrertes rettigheter etter personvernlovgivningen, videreformidles til den behandlingsansvarlige (kunden). Cyberbook kan eventuelt bistå den behandlingsansvarlige med videre håndtering av en henvendelse etter den behandlingsansvarliges forespørsel og nærmere instrukser. Punktene nedenfor gjelder ikke i slike tilfeller.

I tilfeller hvor Cyberbook selv er behandlingsansvarlig, skal henvendelser som vedrører de registrertes rettigheter etter personvernlovgivningen, videreformidles til ledelsen eller den ledelsen har utpekt. Den som behandler henvendelsen, skal loggføre anmodningen med dato, bl.a. for å kunne dokumentere svartid. Hvis anmodningen gjøres muntlig, skal vedkommende nedfelle et skriftlig referat av anmodningen. Den som behandler henvendelsen, skal verifisere at den anmodningen kommer fra, er den registrerte eller handler på fullmakt fra den registrerte.

De registrertes rettigheter omfatter:

- Rett til innsyn, *se punkt 9.2*
- Rett til retting, *se punkt 9.3*
- Rett til sletting, *se punkt 9.4*
- Rett til begrensning av behandlingen, *se punkt 9.5*
- Rett til å protestere mot behandlingen, *se punkt 9.6*
- Rett til dataportabilitet, *se punkt 9.7*

### 9.2 Anmodning om innsyn

1. En Innsynsanmodning skal umiddelbart videreformidles til ledelsen eller den ledelsen har utpekt slik at den kan behandles raskt og senest innen én måned.

2. Hvis Cyberbook behandler personopplysninger om den registrerte, skal Cyberbook gi følgende informasjon til den registrerte:
    a. formålet med behandlingen,
    b. de berørte kategoriene av personopplysninger,
    c. mottakerne eller kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, særlig om opplysningene overføres til land utenfor EØS, samt om de nødvendige garantiene i henhold til GDPR artikkel 46 i forbindelse med overføringen.
    d. dersom det er mulig, hvor lenge det forventes at personopplysningene vil bli lagret, eller, dersom dette ikke er mulig, kriteriene som brukes for å fastsette denne perioden,
    e. retten til å anmode Cyberbook om korrigering eller sletting av personopplysninger eller begrensning av behandlingen av personopplysninger som gjelder den registrerte, eller til å protestere mot behandlingen,
    f. retten til å klage til Datatilsynet,
    g. dersom personopplysningene ikke er samlet inn fra den registrerte, all tilgjengelig informasjon om hvor personopplysningene stammer fra,
    h. At Cyberbook ikke benytter seg av automatiserte avgjørelser, herunder profilering.
3. Dersom den registrerte ber om det, skal det gjøres tilgjengelig en kopi av de personopplysninger som behandles om den registrerte.
4. Det skal sikres at utlevering av personopplysninger ikke medfører at den som ber om innsyn, får innsyn i andre personers personopplysninger.
5. Opplysninger som gjelder forretningshemmeligheter eller på annet grunnlag er underlagt taushetsplikt (overfor andre enn den registrerte), skal sladdes.
6. Cyberbook skal sikre at opplysninger bare utleveres til den som opplysningene gjelder. Hvis det er tvil om det er den registrerte som ber om innsyn, skal ikke opplysningene utleveres inntil dette er avklart. Det skal også sikres at utlevering av personopplysninger ikke gis på en måte som kan medføre risiko for at opplysningene kommer på avveie. Opplysninger som anses som sensitive eller av hensyn til den registrerte krever særskilt beskyttelse, samt alle særlige kategorier personopplysninger, skal ikke sendes på e-post eller på annen måte som ikke sikrer opplysningene tilstrekkelig. Fysisk henting mot fremvisning av ID eller rekommandert brev vil være løsninger som sikrer opplysningenes konfidensialitet.

Det skal ikke kreves gebyr eller annen betaling for oppfyllelse av innsynet, med mindre anmodningen er åpenbart grunnløs eller overdreven, f.eks. ved gjentatte anmodninger. I slike tilfeller kan det kreves et rimelig vederlag basert på Cyberbooks administrative kostnader for å behandle anmodningene, eller anmodningen kan nektes.

## 9.3 Anmodning om retting

1. Anmodningen om retting skal umiddelbart videreformidles til ledelsen eller den ledelsen har utpekt slik at retting kan skje så raskt som mulig.
2. Den som behandler anmodningen, skal undersøke om det er teknisk mulig å foreta rettingen.
3. Om det ikke er noe til hinder for retting, skal rettingen skje uten ugrunnet opphold.

4. Den som behandler anmodningen, skal påse at rettingen blir dokumentert på egnet måte.
5. Cyberbook skal skriftlig bekrefte til den registrerte at rettingen er gjennomført, alternativt at retting ikke er foretatt og årsaken til dette. Den registrerte skal også opplyses om adgangen til å klage til Datatilsynet.

## 9.4 Anmodning om sletting

1. Anmodningen om sletting skal videreformidles til ledelsen eller den ledelsen har utpekt som skal vurdere om sletting kan foretas. Sletting skal ikke foretas om behandling av personopplysningene er nødvendig for å:
   - utøve retten til ytrings- og informasjonsfrihet
   - oppfylle en rettslig forpliktelse som krever behandling i henhold til lovgivningen (f.eks. oppbevaring av regnskapsmateriale)
   - fastsette, gjøre gjeldende eller forsvare rettskrav
2. Om det ikke er noe til hinder for sletting, skal slettingen skje uten ugrunnet opphold.
3. Den som behandler anmodningen, skal påse at rettingen blir dokumentert på egnet måte.
4. Cyberbook skal skriftlig bekrefte til den registrerte at slettingen er gjennomført, alternativt at sletting ikke er foretatt og årsaken til dette. Den registrerte skal også opplyses om adgangen til å klage til Datatilsynet.

## 9.5 Rett til begrensning av behandlingen

1. Anmodningen om begrensning av behandlingen skal videreformidles til ledelsen eller den ledelsen har utpekt som skal vurdere om vilkårene for begrensning foreligger. Det vil være om et av følgende forhold gjør seg gjeldende:
   - den registrerte bestrider riktigheten av personopplysningene, i en periode som gjør det mulig for Cyberbook å kontrollere riktigheten av personopplysningene
   - behandlingen er ulovlig, og den registrerte motsetter seg sletting av personopplysningene og isteden anmoder om at bruken av personopplysningene begrenses,
   - Cyberbook trenger ikke lenger personopplysningene til formålet med behandlingen, men den registrerte har behov for disse for å fastsette, gjøre gjeldende eller forsvare rettskrav
   - den registrerte har protestert mot behandlingen i påvente av en kontroll av om Cyberbooks berettigede interesser går foran hensynet til den registrertes personvern.
2. Om ett av vilkårene angitt ovenfor er oppfylt, skal Cyberbook etterkomme anmodningen og begrense behandlingen tilsvarende.
3. Den som behandler anmodningen, skal påse at begrensningen blir dokumentert på egnet måte.
4. Cyberbook skal skriftlig bekrefte til den registrerte at begrensningen er gjennomført, alternativt at begrensningen ikke er gjennomført og årsaken til dette. Den registrerte skal også opplyses om adgangen til å klage til Datatilsynet.

## 9.6 Rett til å protestere mot behandlingen

1. Protesten mot behandlingen skal videreformidles til ledelsen eller den ledelsen har utpekt som skal vurdere om vilkårene for å protestere er oppfylt. Dette beror på om:
   - Cyberbook behandler personopplysningene på grunnlag av sine (eller en tredjeparts) berettigede interesser, og
   - den registrerte kan vise til "*grunner knyttet til vedkommendes særlige situasjon*" som tilsier at behandlingen skal opphøre.
2. Cyberbook skal i så fall stanse behandlingen med mindre det påvises tvingende berettigede grunner for behandlingen som går foran den registrertes interesser, rettigheter og friheter, eller for å fastsette, gjøre gjeldende eller forsvare rettskrav.
3. Dersom den registrerte protesterer mot behandling med henblikk på direkte markedsføring (f.eks. utsendelse av nyhetsbrev), skal personopplysningene ikke lenger behandles for slike formål.
4. Den som behandler anmodningen, skal påse at opphør av behandlingen, alternativt hvilke tvingende berettigede grunner som foreligger for fortsatt behandling, blir dokumentert på egnet måte.
5. Cyberbook skal skriftlig bekrefte til den registrerte at behandlingen er opphørt, alternativ at den ikke er opphørt og årsaken til dette. Den registrerte skal også opplyses om adgangen til å klage til Datatilsynet.

## 9.7 Dataportabilitet

1. Hvis Cyberbook behandler personopplysninger basert på den registrertes samtykke etter GDPR artikkel 6 nr. 1 bokstav a) eller avtale etter bokstav b), og behandlingen utføres automatisk, har den registrerte rett til å motta personopplysninger om seg selv som vedkommende har gitt til en Cyberbook, i et strukturert, alminnelig anvendt og maskinlesbart format, og rett til å overføre disse opplysningene til en annen behandlingsansvarlig uten at Cyberbook hindrer dette.
2. En anmodning om slik overføring av personopplysninger skal videreformidles til ledelsen eller den ledelsen har utpekt som skal vurdere om vilkårene er oppfylt.
3. Hvis vilkårene er oppfylt, skal Cyberbook så snart som mulig overføre personopplysningene til den registrerte eller den behandlingsansvarlige som den registrerte har utpekt.
4. Den som behandler anmodningen, skal påse at overføringen blir dokumentert på egnet måte.
5. Med mindre overføringen skjer til den registrerte selv, skal Cyberbook skriftlig bekrefte til den registrerte at personopplysningene er overført, alternativt at overføring ikke er skjedd og årsaken til dette. Den registrerte skal også opplyses om adgangen til å klage til Datatilsynet.