Webinar: Hva forventer Datatilsynet av deg når en sikkerhetshendelse har oppstått?

Eirik Gulbrandsen, Senioringeniør
Fredrik Christensen, Seniorrådgiver

Seksjon for teknologi, sikkerhet og tilsyn

Datatilsynet

Hva forventer Datatilsynet av deg når en sikkerhetshendelse har oppstått?

«I foredraget vil Datatilsynet klargjøre i hvilke tilfeller virksomheter må sende avviksmelding, hva som bør meldes når, og når melding ikke er nødvendig. Det vil gis anbefalinger om hva meldingene bør inneholde, med fokus på relevant og viktig informasjon.»

Personopplysningssikkerhet er:

- Sikring av **konfidensialitet (K)**
  - personopplysninger skal ikke bli kjent for uvedkommende

- Sikring av **integritet (I)**
  - personopplysninger ikke kunne bli endret utilsiktet eller av uvedkommende

- Sikring av **tilgjengelighet (T)**
  - personopplysninger er tilgjengelig for autoriserte ved behov

Artikkel 32. Sikkerhet ved behandlingen

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,

c) evne til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstår en fysisk eller teknisk hendelse,

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

Hvorfor melde til Datatilsynet?

Artikkel 33. Melding til tilsynsmyndigheten om brudd på personopplysningssikkerheten

«Ved brudd på personopplysningssikkerheten skal den behandlingsansvarlige uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til vedkommende tilsynsmyndighet … med mindre bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter.»

Hvorfor melde og hvorfor 72 timersfristen?

Sikre at tidsmessig fokus på igangsettelse av tiltak for å redusere konsekvenser for de registrerte skal inngå i virksomhetens hendelseshåndtering. Og det er en lovpålagt forpliktelse…

Artikkel 34. Underretning av den registrerte om brudd på personopplysningssikkerheten

Dersom det er sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet

Hvorfor må vi underrette de berørte?

Informasjon til de berørte - oppsummering

Dersom det er sannsynlig at bruddet vil medføre en høy risiko for de berørtes rettigheter og friheter

- Gi enkeltmennesker mulighet til raskt å igangsette tiltak for å redusere egne konsekvenser av en hendelse.
- Bruk den kanal som det er størst sjanse for å nå ut til den berørte (f.eks. telefon, SMS, e-post, brev..)

Unntak i kravet om varsling:

- Eksisterende tiltak som gjør informasjonen uleselig, f.eks. kryptering
- Tiltak i ettertid som sikrer at den høye risikoen ikke lengre vil oppstå
- Uforholdsmessig innsats. Må i stedet informere offentlig eller tilsvarende.

Håndtering av avvik

Virksomhetenes plikter

Håndtering av avvik

- Meld brudd på personopplysningssikkerheten til Datatilsynet
- Hva er et brudd på personopplysningssikkerheten?
- Hvilke brudd skal meldes til Datatilsynet?
- Hvem kan melde bruddet til Datatilsynet?
- Informasjon til de berørte
- Hvordan følge opp bruddet internt?
- Håndtering av personvernet ved digitale angrep

www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/

Hva gjør man når hendelsen oppstår?

Innhold

Hva gjør dere?

Hvis dere oppdager en pågående sikkerhetshendelse, er det viktig at dere prioriterer håndtering av selve hendelsen og får oversikt over situasjonen:

- Ta i bruk planen deres for krisehåndtering hvis dere har det, og opprett krisestab.
- Vurder å involvere tredjeparter for å håndtere hendelsen hvis dere ikke har kompetanse til å gjøre det selv. Se Nasjonal sikkerhetsmyndighet sin liste over godkjente aktører (nsm.no) og Næringslivets Sikkerhetsråds nødplakat for digitale angrep (nsr-org.no).
- Det finnes en rekke tilbydere av CERT-tjenester Computer Emergency Response Team) som kan være relevante å involvere. Dere finner en oversikt på DFø sine nettsider (markedsplassen.anskaffelser.no).

Dere må også varsle relevante myndigheter:

- På lik linje med Politiet anbefaler vi at datakriminalitet anmeldes (politiet.no).
- Vurder om dere skal varsle Nasjonal sikkerhetsmyndighet (nsm.no).
- Hvis dere mistenker brudd på personopplysningssikkerheten, skal det sendes melding til Datatilsynet innen 72 timer.

Håndtering av brudd og mulig brudd på personopplysningssikkerheten

På nettsidene våre finner dere utfyllende veiledning om når og hvordan dere skal håndtere brudd på personopplysningssikkerheten (avvik).

Oppsummert anbefaler vi at dere ved mistanke om på brudd personopplysningssikkerheten gjør følgende:

1. Iverksetter tiltak for å stoppe selve bruddet.
2. Involverer og søker råd hos personvernombudet deres tidlig i prosessen. Personvernombudet vil også kunne bidra i dialogen med Datatilsynet.
3. Kartlegger hvilke personopplysninger som kan være berørt, vurderer risikoen for de berørte og eventuelt varsler disse.
4. Melder fra til Datatilsynet dersom det er aktuelt.

Hvordan melde brudd på personopplysningssikkerheten (avvik)

Vi vil gjerne at dere bruker Altinn for å melde brudd på personopplysningssikkerheten til oss. Gjennom Altinn får dere tilgang til et skjema hvor vi spør om den informasjonen dere har plikt til å gi oss om bruddet.

Publisert: 24.03.2023
Sist endret: 17.07.2024

- Les om hva et brudd på personopplysningssikkerheten er.
- Les også om hvilke brudd som er meldepliktige.

Vi ber om at dere svarer så detaljert som mulig på de ulike spørsmålene. Nedenfor finner dere hjelp til hva dere skal ha med når dere melder et brudd til oss. Merk at dere også kan legge ved filer gjennom Altinn.

Meld bruddet her (altinn.no)

For dere kan fylle ut skjemaet i Altinn, må dere ha følgende klart:

1. **Tilgang til skjema**
Den som skal melde må ha myndighet til å rapportere inn bruddet på vegne av virksomheten. For å fylle ut og sende inn skjemaet, trengs enten Altinn-rollen «Utfyller/innsender» eller en egendefinert rolle som virksomheten kan opprette.
En egendefinert rolle kan være nyttig dersom virksomheten ønsker å begrense tilgangen for den som skal melde bruddet til enkeltskjemaer. Dersom den som skal melde ikke har en gyldig rolle i Altinn, må den i virksomheten som styrer tilganger kontaktes (disse har rollen "Tilgangsstyring").
Les mer om hvordan du kan gi tilgang til skjema eller tjenester på Altinn.no

2. **Elektronisk ID (eID)**
Den som skal melde trenger en elektronisk ID (eID) for å kunne logge inn i Altinn. Dersom det ikke er ønskelig å bruke private eID, kan virksomheten skaffe et virksomhetssertifikat fra Commfides eller Buypass.

Hva skal man melde (og kanskje ikke melde)

Virksomhetenes plikter

Håndtering av avvik

- Meld brudd på personopplysningssikkerheten til Datatilsynet
- Hva er et brudd på personopplysningssikkerheten?
- Hvilke brudd skal meldes til Datatilsynet?
- Hvem kan melde bruddet til Datatilsynet?
- Informasjon til de berørte
- Hvordan følge opp bruddet internt?
- Håndtering av personvernet ved digitale angrep

Når den behandlingsansvarlige opplever et brudd på personopplysningssikkerheten, må det vurderes hvilken *risiko* bruddet innebærer for de berørte personenes rettigheter og friheter.

Den behandlingsansvarlige trenger ikke melde bruddet til Datatilsynet dersom «bruddet sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter» (art 33).

Den behandlingsansvarlige må være tilnærmet helt sikker på at bruddet ikke vil medføre eller har medført noen risiko for de berørte, for at unntaket skal være oppfylt. Hvis den behandlingsansvarlige er usikker på om unntaket er oppfylt, er det bedre å melde til Datatilsynet for sikkerhets skyld.

Scenario - konfidensialitet

Hos et sykehus tas det røntgenbilder av en pasient. Pasienten har i etterkant av røntgenundersøkelsen blitt henvist til en spesialist i kommune-helsetjenesten. Ved en menneskelig feil har legen ved sykehuset sendt røntgenbildene til feil spesialist.

Spesialisten som er mottaker av de feilsendte røntgenbildene melder selv fra til sykehuset, og bekrefter at bilder og opplysninger er slettet.

Ikke meldepliktig

På et sykehus utføres det judisiell vurdering av en person, for å avklare om hen som siktet i en straffesak har noen av de psykiske tilstandene som betinger straffefrihet og/eller forvaring.

Rapporten fra den kliniske vurderingen sendes som vanlig elektronisk over til relevant rettsinstans.

Ansvarlig for oversendelsen glemmer å merke saken som unntatt offentlighet. Sykehusets offentlige postliste inneholder dermed en post som ser slik ut:

- *Sykehus X, Psyk.avd – Judisiell vurdering av Ola Nordmann - xx.xx.2024*

Meldepliktig

Scenario - Integritet

Et entreprenørfirma har en database som inneholder opplysninger om alle deres kunder. Firmaet har fått ny IT-tjenesteleverandør og skal migrere sine databaser over til ny plattform.

Personell i administrasjonen oppdager at tabellen som inneholder telefonnummer og adresse til kontaktpersoner hos kundene er feil etter migrasjonen.

Tjenesteleverandøren retter feilen ved å gjøre en ny migrering fra tidligere miljø.

Ikke meldepliktig

En lege skal melde inn dødsfall elektronisk. Dødsmeldingen sikrer at personopplysningene blir sendt til Folkeregisteret, og person- og helseopplysninger blir sendt Dødsårsaksregisteret. Legen registrerer dødsmeldingen på feil person.

Folkeregisteret oppdateres umiddelbart og det betyr at mange av den registrertes tjenester vil bli avsluttet innen kort tid, som for eksempel BankID, banktjenester og NAV-tjenester.

Meldepliktig

Scenario - Tilgjengelighet

Et skole opplever at nettsidene er nede for en kortere perioden og identifiserer årsaken til å være et tjeneste-nektangrep (DDoS). Nettsidene blir tilgjengelig igjen etter at angrepet avsluttes.

Ikke meldepliktig

Et apotek som leverer publikumstjenester har nedetid på et sentralt system grunnet teknisk svikt hos en underleverandør. Nedetiden medfører at apoteket ikke får ekspedert resepter. Ingen opplysninger er på avveier men reseptekspedisjonen i apoteket er ikke operativ.

Meldepliktig

Hva bør meldingene inneholde

Kontekst er viktig

- Meldinger om brudd skal fokusere på mulige konsekvenser for fysiske personer
- Informasjon i meldingen skal gi tilstrekkelig grunnlag for at Datatilsynet kan vurdere alvorlighetsgrad og sannsynlighetsvurdering
- Omfang og type opplysninger er viktig
- Beskrivelse av pågående og planlagte tiltak er vesentlig for situasjonsvurdering

- **Gi gjerne en egen vurdering, men den skal underbygges/dokumenteres med fakta:**
  - «Vi tror ikke informasjon ble kopiert ut av filserver»
    - Hva underbygger denne antagelsen? Logger, nettverkstrafikk, analysetrafikk?
  - «Personopplysninger var ikke en del av informasjonen som ble kopiert»
    - Hva underbygger denne antagelsen? Oversikt over dokumenter med klassifisering av informasjonen?

- **Midlertid informasjon er tilstrekkelig (innen 72-timersfristen) - midlertidig melding**
  - Må fremdeles inneholde tilstrekkelig informasjon til foreløpig vurdering av alvorlighet, evt. beskrivelse av hva som er ukjent
    - «Vi har en filserver som bl.a. inneholder ansatte sykemeldinger, men vet ikke om denne var omfattet av hendelsen».
  - Må beskrive planlagte aktiviteter for videre oppfølging og tidsplan
  - Det forventes en oppdatering innen senest en måned etter midlertidig melding, hvis ikke får den status «ufullstendig melding» med risiko som «uavklart, men potensiell høy» → kan/vil utløse krav om redegjørelse

Hva bør meldingene inneholde forts.

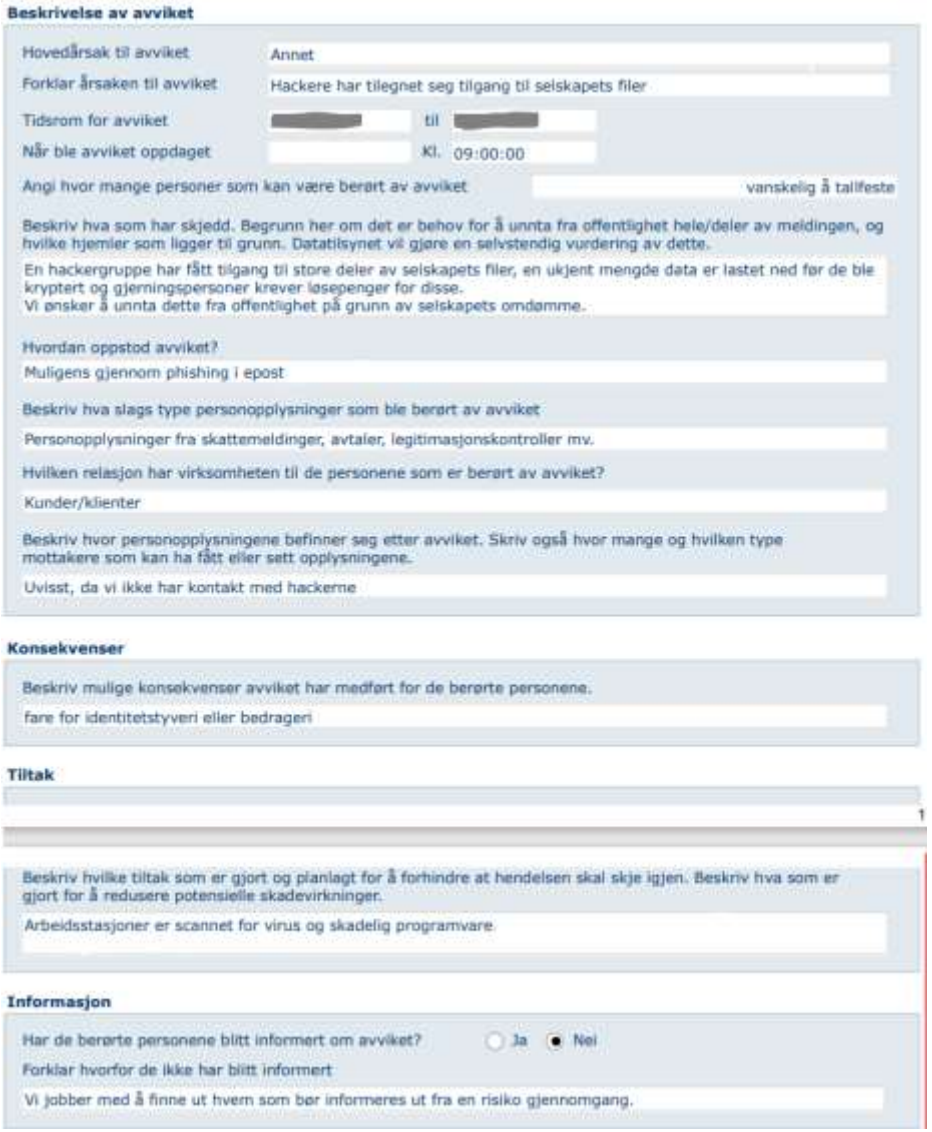
- Om undersøkelser har fastslått om opplysninger faktiske har kommet på avveie, eventuelt dokumentasjon av hvorfor man mener dette ikke er tilfelle.
- Hvilke tiltak er igangsatt for å redusere risiko for de berørte.
- Gjenganger: «Vi har ikke grunnlag for å si at personopplysninger er på avveier, men kan heller ikke utelukke det».
  - Hvilke tiltak er igangsatt for å avklare status
- Det ønskes også en status på om eventuelt registrerte er informert.

Hva bør meldingene ikke inneholde

- Direkte personopplysninger (utover kontaktperson)
- Også «indirekte personopplysninger»
  - «Kommunens saksbehandler for byggesaker»
- Detaljerte beskrivelser av teknisk plattform og arkitektur (inkl. IP-adresser)
- Detaljerte beskrivelser av tekniske sikkerhetsløsninger (inkl. produktnavn)
  - Dette er informasjon vi eventuelt etterspør ved behov

- Generelt informasjon som ikke er relatert til risiko for de berørte
  - Konsekvenser for virksomheten og eventuelt andre virksomheter (såfremt den ikke er relevant for personopplysningsssikkerheten)

For lite informasjon? → Krav om redegjørelse



Beskrivelse av avviket

Hovedårsak til avviket: Annet

Forklar årsaken til avviket: Hackere har tilegnet seg tilgang til selskapets filer

Tidsrom for avviket: [redacted] til [redacted]

Når ble avviket oppdaget: Kl. 09:00:00

Angi hvor mange personer som kan være berørt av avviket: vanskelig å tallfeste

Beskriv hva som har skjedd. Begrunn her om det er behov for å unnta fra offentlighet hele/deler av meldingen, og hvilke hjemler som ligger til grunn. Datatilsynet vil gjøre en selvstendig vurdering av dette.

En hackergruppe har fått tilgang til store deler av selskapets filer, en ukjent mengde data er lastet ned før de ble kryptert og gjerningspersoner krever løsepenger for disse.
Vi ønsker å unnta dette fra offentlighet på grunn av selskapets omdømme.

Hvordan oppstod avviket?

Muligens gjennom phishing i epost

Beskriv hva slags type personopplysninger som ble berørt av avviket

Personopplysninger fra skattemeldinger, avtaler, legitimasjonskontroller mv.

Hvilken relasjon har virksomheten til de personene som er berørt av avviket?

Kunder/klienter

Beskriv hvor personopplysningene befinner seg etter avviket. Skriv også hvor mange og hvilken type mottakere som kan ha fått eller sett opplysningene.

Uvisst, da vi ikke har kontakt med hackerne

Konsekvenser

Beskriv mulige konsekvenser avviket har medført for de berørte personene.

fare for identitetstyveri eller bedrageri

Tiltak

Beskriv hvilke tiltak som er gjort og planlagt for å forhindre at hendelsen skal skje igjen. Beskriv hva som er gjort for å redusere potensielle skadevirkninger.

Arbeidsstasjoner er scannet for virus og skadelig programvare

Informasjon

Har de berørte personene blitt informert om avviket? ○ Ja ● Nei

Forklar hvorfor de ikke har blitt informert

Vi jobber med å finne ut hvem som bør informeres ut fra en risiko gjennomgang.

Vi ber om en oppdatering av sakens status og med spesielt med to fokus;

1. En nærmere beskrivelse av hvilke type personopplysninger med fokus på personopplysninger med særskilt beskyttelsesbehov som potensielt kan ha kommet på avveie, samt en vurdering av risiko for de registrerte om informasjonen skulle ha kommet på avveie. Og om granskning har fastslått om opplysninger faktiske har kommet på avveie, eventuelt dokumentasjon av hvorfor man mener dette ikke er tilfelle. Det ønskes en kort beskrivelse av hvilke verktøy og metoder som er benyttet for å underbygge eventuelle konklusjoner. Det ønskes også en status på om eventuelt registrerte er informert.

2. En kort beskrivelse av om interne styringssystemer (internkontroll/risikovurderinger) for informasjonssikkerhet og personopplysningssikkerhet er benyttet i perioden avviket gjelder. Det bes ikke om dokumentasjon på selve styringssystemene, kun om dette har vært benyttet som styringsverktøy i perioden. Hvis styringssystemer har vært benyttet, en vurdering av hvorfor disse ikke har fanget opp situasjonen tidligere.

Vi ber om et svar på denne henvendelsen senest xx. oktober 20xx. Saken kan oppdateres som tilleggsmelding via samme kanal som opprinnelig melding om brudd på personopplysningssikkerheten.

Selve saksbehandlingen – hva vurderer vi?

Har virksomheten meldt inn det som kreves og forventes, jf kravene etter artikkel 33 og vår veiledning?

- Hovedårsak
- Tidsrom
- Når ble avviket oppdaget
- Antall berørte personer
- Hva som har skjedd
- Hvordan avviket oppstod
- Hva slags type personopplysninger som ble berørt
- Hvilken relasjon virksomheten har til de berørte personene
- Hvor personopplysningene befinner seg etter avviket
- Mulige konsekvenser avviket har medført for de berørte personene
- Hvilke tiltak som er gjort og planlagt for å hindre gjentakelse, og hva som er gjort for å redusere potensielle skadevirkninger
- Har de berørte personene blitt informert, eller vil de bli det? Hvordan? (art 34)
- Navn og kontaktinformasjon til *personvernombud* eller kontaktperson hos virksomheten som kan gi mer informasjon om avviket.

Saksbehandlers vurderinger

- Gikk det lang tid før hendelsen ble oppdaget og deretter meldt til Datatilsynet?
- Er det mulig å foreta en vurdering av alvorlighetsgrad basert på informasjon i meldingen?
- Hvor alvorlige er konsekvensene for registrertes rettigheter og friheter, og er det mange berørte?
- Konteksten personopplysningene er blitt behandlet (type virksomhet, kategorier personopplysninger og registrerte)
- Indikerer bruddet alvorlige mangler i internkontroll og informasjonssikkerhet?
- Har virksomheten hatt tilsvarende brudd tidligere?
- Er de igangsatte tiltakene tilstrekkelige og effektive?
- Er det gitt tilstrekkelig informasjon til de registrerte?

→ indikasjoner på at virksomheten ikke har forstått sitt ansvar
→ indikasjoner på at virksomheten ikke har lært (av denne og eventuelt tidligere hendelser)

Hvordan følger vi opp?

- Vurderer om saken er tilstrekkelig opplyst og håndtert – vurdere avslutning
- Tar eventuelt kontakt muntlig for å ta enkle avklaringer
- Sender skriftlig krav om redegjørelse
  - Skriftlig krav om redegjørelse er i seg selv ikke negativt, men et ønske om tilstrekkelig beslutningsunderlag (også for å avslutte saker)
- Vurderer om saken gir grunnlag for å vurdere tilsyn med virksomheten (stedlig besøk)
- Fatter en beslutning, eventuelt et vedtak

postkasse@datatilsynet.no
Telefon: +47 22 39 69 00

datatilsynet.no
personvernbloggen.no