Krav til informasjonssikkerhet i nytt personvernregelverk

Personvernkonferansen

Eirin Oda Lauvset | seniorrådgiver

8. desember 2017

Datatilsynet

Informasjonsikkerhet er et ledelsesansvar

- Sikkerhetsledelse
- Klare ansvarsforhold
- Oversikt over det totale risikobildet og beslutte mål

Styring av informasjonssikkerhet handler om:

- Verdier
- Sikkerhetsmål
- Risiko som skal enten
  -fjernes – reduseres - aksepteres

Roller og ansvar er tydeliggjort

Direktiv/ personopplysningslov

- ❑ Behandlingsansvarlig, forskriftens §§ 2-3, 2-4 2.ledd, 2-7 og kapittel 3 om internkontroll.
- ❑ Databehandler, forskriftens § 2-15 3.ledd (kun informasjonssikkerhet)

Forordning

- ❑ Eksplisitte krav til både DB og BA.
- ❑ Behandlingsansvarlig kan kun velge databehandlere som viser at de skal iverksette tiltak slik at loven følges (f.eks. følger bransjenorm)
- ❑ Loven gjelder direkte for databehandlere, bl. annet:
  - Plikt til å sørge for informasjonssikkerhet
  - Plikt til å dokumentere
  - Plikt til å bistå behandlingsansvarlig i avvikssaker
  - Sanksjoner
  - Erstatningsansvar

Nøkkelen til etterlevelse (*accountability*)?

Artikkel 5 (2) 'accountability'
Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at personvernprinsippene overholdes (inkl. info.sikkerhet)

- Mindre forhåndskontroll – bortfall av melde- og konsesjonsplikt
- Flere (og til dels tydeligere) rettigheter og plikter
- Risikobaserte tiltak (DPIA, forhåndsdrøftelse, etterkontroll)
- Strengere sanksjoner

Informasjonssikkerhet som grunnprinsipp

- **Artikkel 5 (1) f '*integrity and confidentiality*'**

Personopplysninger skal

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

Krav til informasjonssikkerhet er tatt inn som et grunnprinsipp for behandling av personopplysninger – hva betyr det?

Internkontrollplikt i artikkel 24

Identifisere
- Roller
- Opplysninger
- Formål
- Kilder
- Mottakere
- Begrensninger

Gjennomføre
- Risikovurdering
- Tekniske tiltak
- Organisatoriske tiltak

Oppdatere
- Revisjon, test, etc

Dokumentere
- Oversikt jf. art 30
- Bransjenormer/ sertifisering

Informasjonssikkerhet – tekniske og organisatoriske tiltak

Hva er informasjonssikkerhet?

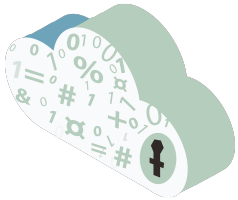
- Sikring av konfidensialitet
  -at informasjon ikke blir kjent for uvedkommende
- Sikring av integritet
  -at informasjon ikke blir endret utilsiktet eller av uvedkommende
- Sikring av tilgjengelighet
  -at informasjon er tilgjengelig for autoriserte ved behov
- Nytt etter forordningen: **robusthet**
  -organisasjonen og systemers evne til å gjenopprette normaltilstand

Sikkerhet ved behandling – art. 32

Idet det tas hensyn til det 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 i forhold til risikoen, […]"*

Tilfredsstillende sikkerhet skal bedømmes ut ifra kontekst – art. 32

Behandlingsansvarlig skal

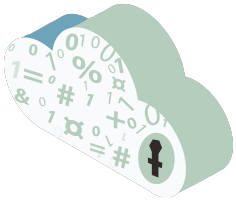


- **Gjøre en risikovurdering**
  kartlegge risikoene av varierende sannsynlighet og alvorlighetsgrad for fysiske personers rettigheter og friheter

…hvor følgende kan hensyntas:

- State of the art – den til enhver tid tilgjengelige teknologi
- Gjennomføringskostnader
- Behandlingens art, omfang, formål og sammenhengen den utføres i

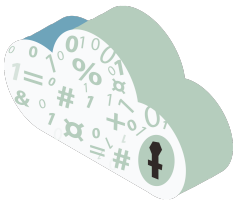
Sikkerhet ved behandling – art. 32



Sikkerhetstiltak

- Pseudonymisering og kryptering av personopplysninger
- Sikre vedvarende fortrolighet (konfidensialitet), integritet, tilgjengelighet og robusthet
- Gjenoppretting av tilgjengelighet og tilganger ved hendelser
- Jevnlig testing, vurdering og evaluering

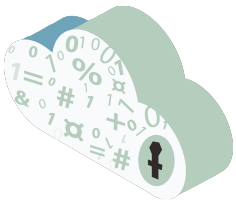
Sikkerhet ved behandling – art. 32



Organisatorisk sikkerhet

- Måten virksomheten er organisert – personer og rutiner
- Instrukser i hvordan oppgaver skal løses for å sikre vedvarende fortrolighet (konfidensialitet), integritet, tilgjengelighet og robusthet
- Bygge sikkerhetskultur

Sikkerhet ved behandling – art. 32



Oppnådd sikkerhet må verifiseres

Art 32 (1) d
"en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er»

Eksplisitt krav om at sikkerheten skal testes
– tekniske og organisatoriske tiltak – virker de?

Sikkerhet ved behandling – art. 32

Etterlevelse skal dokumenteres

❑ Internkontroll
-protokoller over behandlingsaktiviteter (art. 30)
-risikovurderinger (art. 24, 25, 32, 35)
-beskrevne tiltak og dokumentasjon på at de er fulgt opp
-innebygd personvern (art. 25)
-DPIA (art. 35)
-avvikshåndtering (art. 33-34)

❑ Bransjenormer eller godkjent sertifiseringsordning

❑ Tiltak for å sørge for at behandling kun skjer på instruks fra behandlingsansvarlig

Oppsummert

❑ Tilfredsstillende informasjonssikkerhet = **aktsomhet**

Sentrale elementer for aktsomhetsvurderingen:

- Har du tatt hensyn til **moderne teknologi** og metode når sikkerhetskrav ble satt?

- Har du kartlagt vurdert hvilken **type opplysninger virksomheten behandler, omfang, sammenheng og formål**?

-Har du sett **kostnaden** for sikkerhetstiltak i sammenheng med kontekst?

- Har du iverksatt et system som gjør det mulig for deg å måle om de sikkerhetstiltakene du har bestemt faktisk **fungerer** etter planen?

Avviksmeldinger til DT og informasjon til berørte

Avvikshåndtering og avviksmelding (artikkel 33 og 34)

- I dagens regelverk finnes en plikt til å sende avviksmelding til Datatilsynet, dersom avviket har medført *uautorisert utlevering av personopplysninger som krever konfidensialitet* (personopplysningsforskriften § 2-6 tredje ledd)

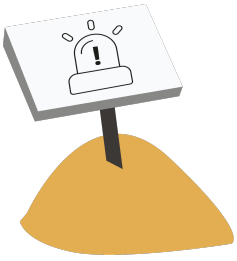
- I personvernforordningen videreføres plikt til å sende avviksmelding til Datatilsynet, men
  - bredere nedslagsfelt,
  - reglene er med detaljerte enn i dag,
  - bestemmelsene regulerer eksplisitt plikt til å informere berørte

- **Dette er endringer som åpenbart må føre til endrede rutiner hos virksomhetene.**

Avviksmeldinger – art. 33

Når må virksomheten sende melding om avvik til Datatilsynet?

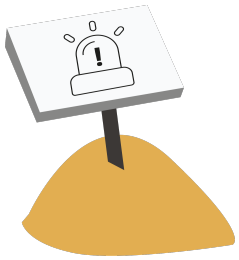
«Ved brudd på personopplysningssikkerheten …, med mindre det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter.»



Definisjon: *«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* (art. 4 (12)

Ikke bare konfidensialitet, men også tilgjengelighet og integritet

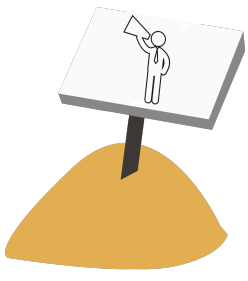
Avviksmeldinger – art. 33



- Behandlingsansvarlig må melde avvik innen 72 timer. Kan meldes trinnvis.
- Databehandler melder til behandlingsansvarlig
- Krav til innholdet i avviksmeldingen (nr 3 a-d)
- Datatilsynet har utarbeidet skjema som tar inn obligatorisk informasjon. Europeisk initiativ til felleseuropeisk skjema.

Informasjon til de berørte – art. 34

- Kravet finnes ikke eksplisitt i dagens regelverk, men i forvaltningspraksis
- GDPR: Berørte skal informeres så raskt som mulig, slik at de skal kunne foreta seg noe for å begrense skaden.
- 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.



Avviksmelding – veiledningsmateriell


Veileder

Virksomhetens ansvar etter nytt regelverk

Nye krav til avvikshåndtering og informasjon til de berørte

Med de nye reglene som trer i kraft i mai 2018 skal mange flere sikkerhetsbrudd eller hendelser rapporteres.

Publisert: 13.08.2017

I dagens regelverk stilles det krav til at avvik eller sikkerhetsbrudd skal håndteres internt i virksomheten. Datatilsynet skal varsles dersom det har vært en «uautorisert utlevering av personopplysninger som krever Avvikfilmsnyttje (personopplysningsforskriften § 2-6). Per i dag er det stort sett saker der det har vært en utlevering av konfidensielle personopplysninger som rapporteres.

Et sikkerhetsbrudd defineres som 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.

Strengere krav til varsling

Fra 2018 blir det strengere krav til når avvik skal rapporteres til Datatilsynet. Den behandlingsansvarlige får frist på å melde fra om sikkerhetsbrudd innen 72 timer etter at den har fått kjennskap til bruddet. Det er også et nytt krav at databehandlere umiddelbart skal varsle behandlingsansvarlige dersom de oppdager et avvik. Dersom virksomheten ikke har full oversikt over sikkerhetsbruddet, kan avviksmeldingen sendes inn trinnvis. Avvikshåndteringen skal dokumenteres også hos virksomheten.

Det stilles i tillegg krav til hva avviksmeldingen til Datatilsynet skal inneholde. Innlevering av avviksmeldinger gjøres digitalt eller per post. Vårt digitale skjemaet tar høyde for kravene til innhold som gjelder fra 2018.

Kravene knyttet til avvik finner du i artikkel 33, mens definisjonen på et sikkerhetsbrudd står i artikkel 4.

Varsling av de berørte

Forordningen gir regler for når de som er berørt av et sikkerhetsbrudd skal varsles og hva det skal inneholde. Varsling skal skje når det er sannsynlig at avviket vil medføre en høy risiko for personvernet til de som er berørt. Varsel skal gis så fort som mulig. Det skal ha et klart og forståelig språk tilpasset leserens nivå.

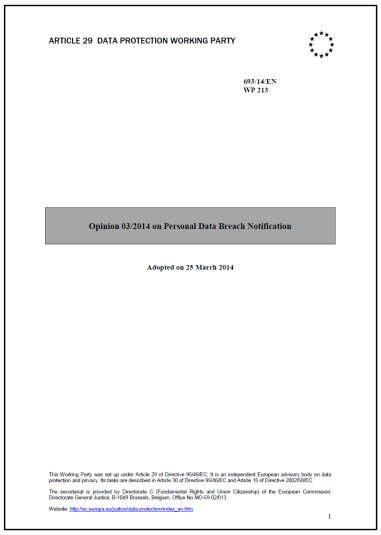
Varselet skal som et minimum inneholde:

1. en beskrivelse av avvikets natur
2. kontaktinformasjon til personvernombudet eller annet kontaktpunkt i virksomheten
3. en beskrivelse av mulige konsekvenser av avviket

Se Datatilsynets veiledning på våre nettsider

https://www.datatilsynet.no/regelverk-og-skjema/veiledere/virksomhetens-ansvar-etter-nytt-regelverk/

WP 29-gruppen har nå oppdatert veileder på høring.
(Blir tilgjengelig fra våre DTs nettsider)


ARTICLE 29 DATA PROTECTION WORKING PARTY

693/14/EN
WP 213

Opinion 03/2014 on Personal Data Breach Notification

Adopted on 25 March 2014

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental Rights and Union Citizenship) of the European Commission, Directorate General Justice, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm

1

Innebygd personvern og personvern som standardinnstilling

Tech

Flashlight app kept users in the dark about sharing location data: FTC

By Cecilia Kang December 5, 2013 Follow @ceciliakang

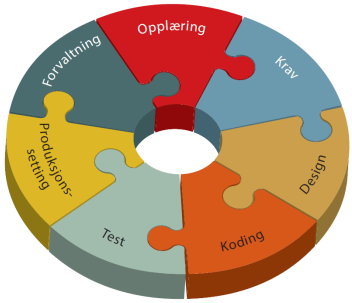
Up to 100 million users downloaded a popular Android app that turned their phones into flashlights. What they didn't realize was that their smartphones also became sophisticated tracking devices, with the app collecting information that could pinpoint their precise location.

The Federal Trade Commission on Thursday issued its first enforcement action related to location-based technology, reaching a settlement with the maker of Brightest Flashlight Free for allegedly hiding the fact that it sold information about the location of its users and the unique string of numbers assigned to a device.

Kilde: http://www.washingtonpost.com/business/technology/flashlight-app-kept-users-in-the-dark-about-sharing-location-data-ftc/2013/12/05/1be26fa6-5dc7-11e3-be07-006c776266ed_story.html

Innebygd personvern og personvern som standard - art 25

- Obligatorisk for informasjonssystemer som bygges etter ikrafttreden av forordningen
- Tekniske og organisatoriske tiltak for å ivareta personvernprinsippene og de registrertes rettigheter
- Tekniske og organisatoriske tiltak for å sikre at prinsippet om dataminimering gir føring på standardinnstillinger



Risikovurdering

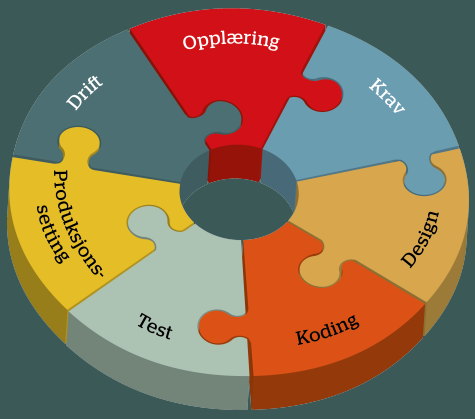
- Kartlegging av verdier – personopplysninger
- Trusselvurdering
- Vurdering av om verdiene er sårbare for truslene
- Resultat = toleransenivå?
- Tiltak for å redusere risiko

Vurdering av personvernkonsekvenser

Ivaretar programvaren den registrertes rettigheter?

Balansere:

- Åpenhet
- Ikke kobling av data
- Mulighet til å gripe inn
- Konfidensialitet
- Integritet
- Tilgjengelighet



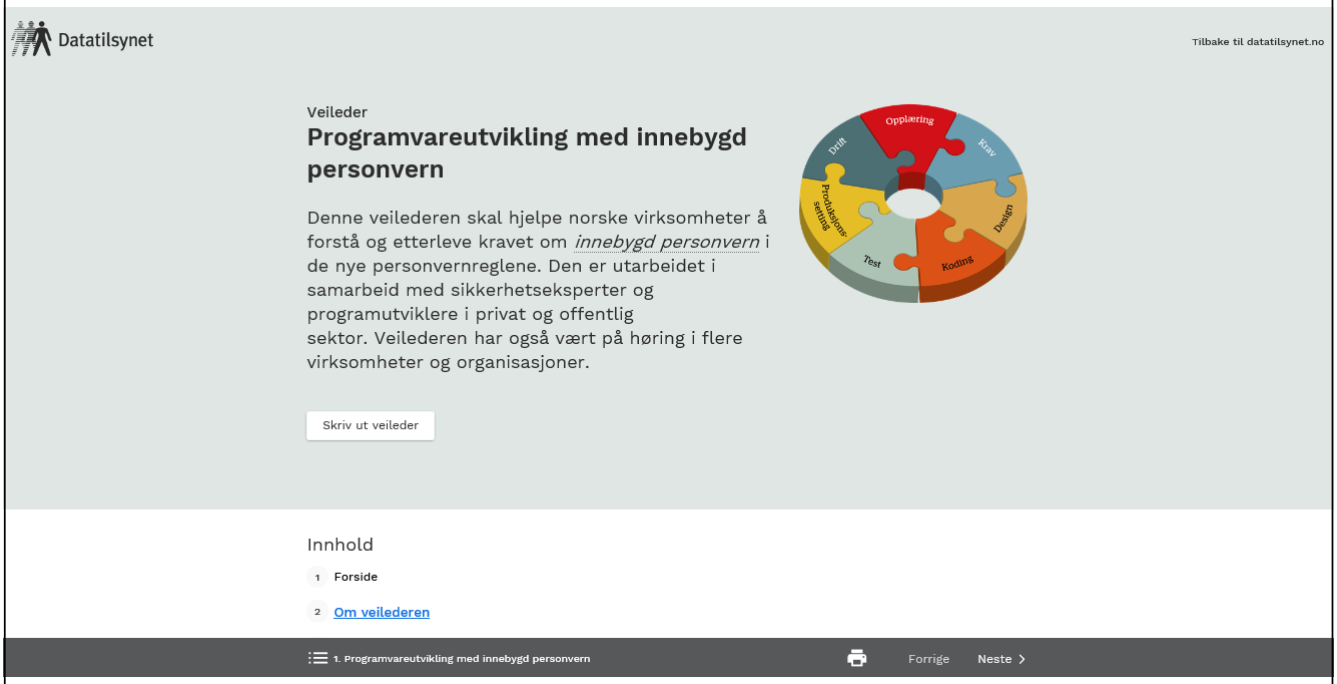
Datatilsynets veileder i innebygd personvern

Personvern- og sikkerhetskrav

Type personopplysninger?
Kan slutninger trekkes om individer?
Hvem er brukere og eiere?
Behandlingsansvarlig, databehandler, mottaker?

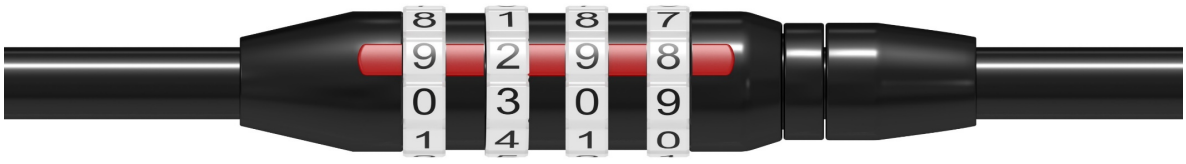
- Prinsipper skal være oppfylt og rettigheter ivaretatt
- Nødvendig? Mengde, omfang, lagringstid, tilgjengelighet
- Åpenhet – gi informasjon så den registrerte kan ivareta sine rettigheter
- Informasjonssikkerhet

Veilederen ligger på datatilsynet.no



Forskjeller og likheter – internkontroll og info.sikkerhet

- Internkontroll og informasjonssikkerhet er viktig i begge regelverk.
- Risikobasert tilnærming, som er viktig også i dagens regelverk, forsterkes i nytt regelverk.



Forskjeller og likheter – internkontroll og info.sikkerhet

- Sentralt poeng: Sammenliknet med dagens bestemmelser om informasjonssikkerhet og internkontroll, legger GDPR og ansvarlighetsprinsippet et større press på
  - virksomhetsbaserte vurderinger om hva som er tilstrekkelig og adekvat med utgangspunkt i sine utfordringer, risiko, mengde og følsomhet av personopplysninger, osv.
  - påvise/demonstrere regeletterlevelse
- Behov for kunnskap, systematikk, gode beslutningsprosesser og dokumentasjon

Takk for oppmerksomheten!

Datatilsynet

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

datatilsynet.no
personvernbloggen.no

eol@datatilsynet.no | @EirinOda (Twitter)