Nye personvernregler (GDPR)

NOKIOS 2017

Martha Eike | senioringeniør

02.11.2017

Datatilsynet

- Bakgrunn
- Ansvarlighet og internkontroll
- Informasjonssikkerhet og avviksmeldinger
- Vurdering av personvernkonsekvenser (DPIA) og forhåndsdrøftelse
- Innebygd personvern

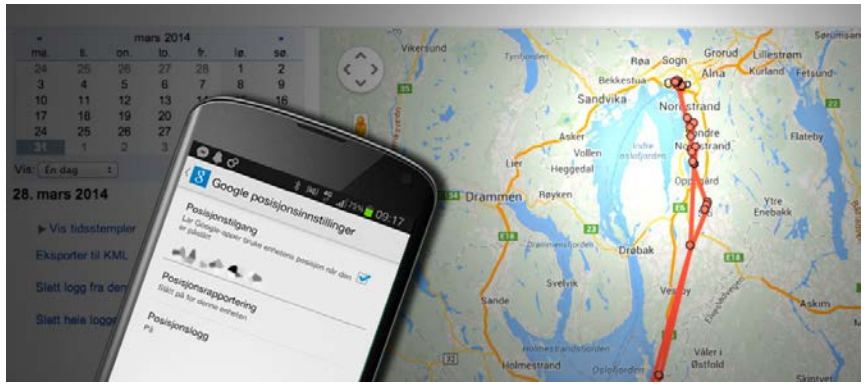
Personvern og definisjoner

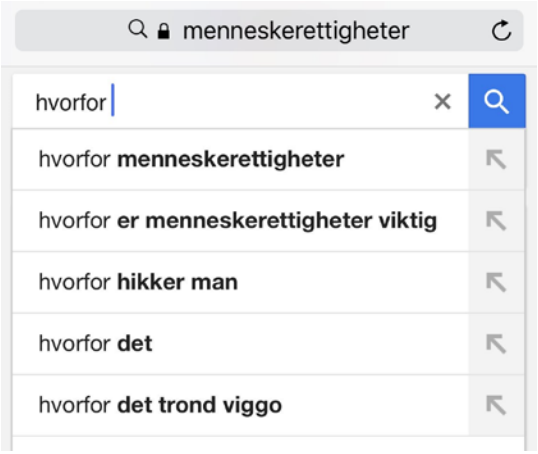
Personopplysninger – hva er det?

Peder Aas
2020 Lillevik

F.nr 180262 34997

Fødselsnummer: 13087846271
Telefonnummer: 22396900
IP-adresse: 195.159.103.82
Bilnummer: BL 23456
Bluetooth MAC: 17:35:52:78:4B:CA
Wi-Fi-adresse MAC: 12:44:32:45:7B:C9
Autpass-brikke-ID: 7483920983278394
UDID: f7426bd759856431d9ae2c99175407a0dcd67ab5



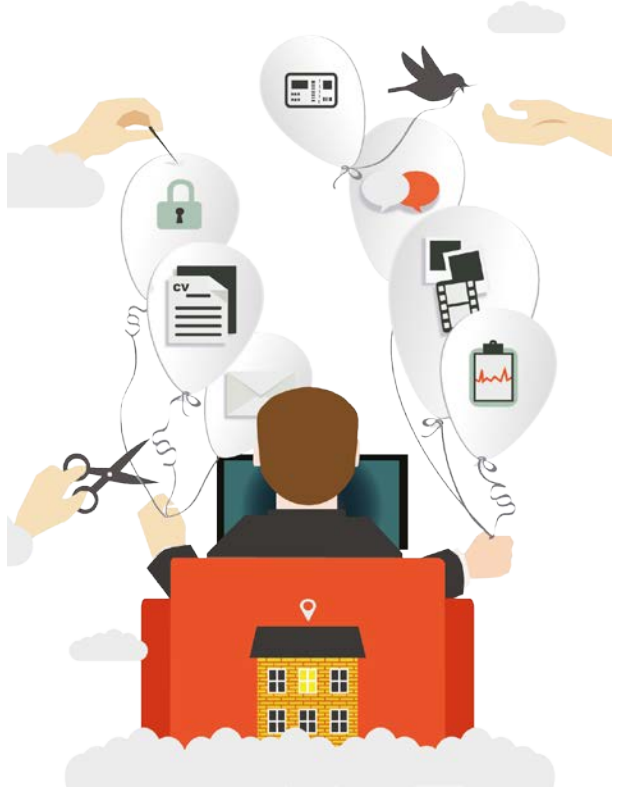


Hva er person(opplysnings)vern?

”Den enkeltes rett til å ha kontroll med egne personopplysninger”

Selvbestemmelse – rett til selv å bestemme hvilke opplysninger som skal brukes, av hvem, til hvilke formål.

Informasjon – hvis man ikke har rett til å samtykke, har man i det minste rett til å vite hvilke opplysninger som brukes, av hvem og til hvilke formål



Prinsipper for behandling av personopplysninger

- Lovlig, rettferdig og gjennomsiktig
- Formålsbegrensning
- Dataminimering
- Riktighet
- Lagringsbegrensning
- Integritet og konfidensialitet
- Ansvarlighet

De registrertes rettigheter

- Informasjon
- Innsyn
- Korrigering
- Sletting
- Begrensning
- Dataportabilitet
- Innsigelse
- Automatiserte avgjørelser, inkludert profilering

Ansvarlighet og internkontroll

Nøkkelen til etterlevelse (*accountability*)?

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

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

Source: LinkedIn

Plikter for behandlingsansvarlige og databehandlere

- Den behandlingsansvarliges ansvar (Art. 24)
- Protokoll over behandlingsaktiviteter (Art. 30)
- Vurdering av personvernkonsekvenser (Art. 35)
  - Forhåndsdrøftelser (Art. 36)
- Innebygd personvern (Art. 25)
- Sikkerhet (Art. 32)
  - Avviksmeldinger (Art. 33) og informasjon til de berørte (Art. 34)
- Databehandlere (Art. 28)
  - Innhold i databehandleravtale (Art. 28 (3))
- Personvernombud (Art. 37-39)
- Atferdsnormer (Art. 40-41)
- Sertifisering (Art. 42-43)

Internkontroll og ansvar

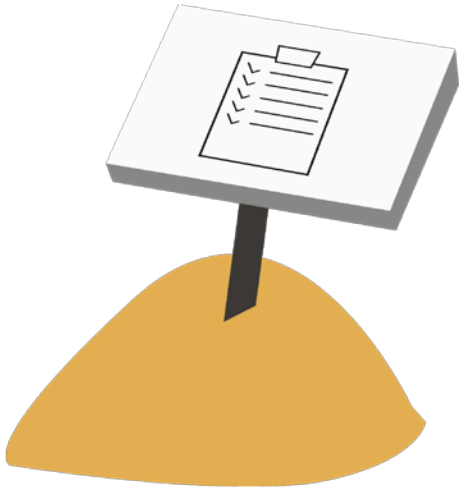
Finnes i personopplysningsloven i dag som **planlagte og systematiske tiltak** i pliktene om internkontroll og informasjonssikkerhet.
(personopplysningsloven §§ 14 og 13)

Artikkel 24 'Den behandlingsansvarliges ansvar'

- Forholdsmessighet
  - Art, omfang, formål og sammenheng
  - Risiko for rettigheter og friheter
- Egnede tekniske og organisatoriske tiltak
  - Etablere og ta i bruk nødvendige rutiner for vern av personopplysninger
- Sikre og dokumentere etterlevelse
- Kontinuerlig prosess

Oversikt over behandlingsaktiviteter – art. 30

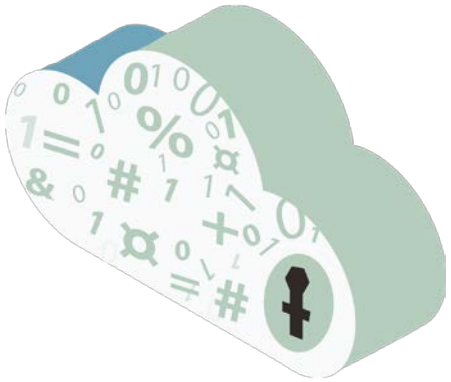
- Kontaktinformasjon til behandlingsansvarlig
- Formål
- Kategorier av registrerte og personopplysninger
- Kategorier av mottakere
- Evt. overføringer til tredjeland
  eller internasjonale organisasjoner,
  og dokumentasjon på tilstrekkelig
  beskyttelse
- Slettefrister
- Sikkerhetstiltak

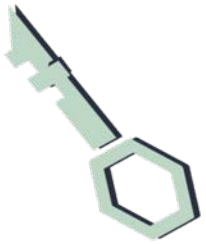


Databehandlere skal ha tilsvarende oversikt over det de gjør på vegne av ulike behandlingsansvarlige

Informasjonssikkerhet og avviksmeldinger

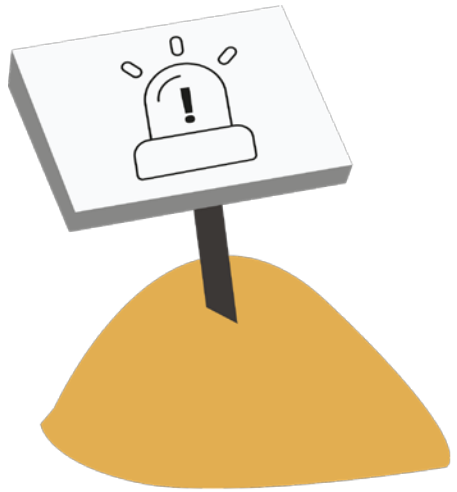
Sikkerhet ved behandling – art. 32





- Risikovurdering
- Sikkerhetstiltak
  - Pseudonymisering og kryptering av personopplysninger
  - Sikre vedvarende K, I, T og robusthet
  - Gjenoppretting av tilgjengelighet og tilganger ved hendelser
  - Jevnlig testing, vurdering og evaluering
- Bransjenormer eller godkjent sertifiseringsordning
  - Element for å vise etterlevelse
- Tiltak for å sørge for at behandling kun skjer på instruks fra behandlingsansvarlig

Avviksmeldinger – art. 33 og 34



- Ved brudd på personopplysningssikkerheten – både konfidensialitet, integritet og tilgjengelighet
- Behandlingsansvarlig må melde avvik innen 72 timer. Kan meldes trinnvis.
- Databehandler melder til behandlingsansvarlig
- Stilles krav til innholdet i avviksmeldingen. Vårt skjema i Altinn tar høyde for dette.
- Berørte skal informeres så raskt som mulig, slik at de skal kunne foreta seg noe for å begrense skaden.
- Veiledning fra Artikkel 29-gruppen om artikkel 33 og 34.

Vurdering av personvernkonsekvenser (DPIA) og forhåndsdrøftelse

Vurdering av personvernkonsekvenser - Privacy / Data protection impact assessment (PIA/DPIA)

En systematisk prosess, som...

identifiserer og evaluerer...

fra alle interessenters synsvinkel...

potensielle personvernkonsekvenser i...

et prosjekt, initiativ, foreslått system eller prosess...

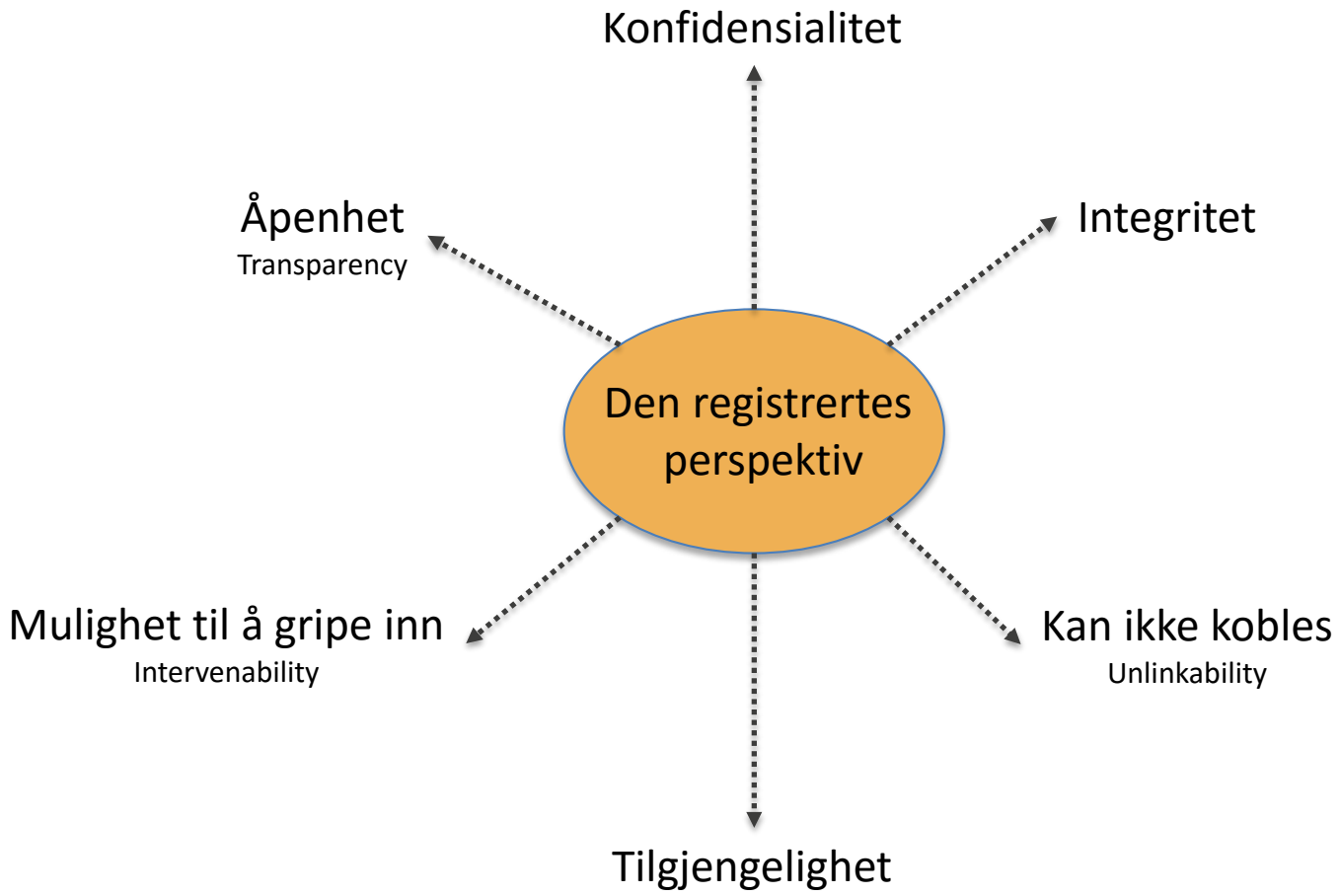
og som inkluderer det å finne ut...

hvordan dere kan unngå trusler mot personvernet...

eller

hvilke tiltak dere må innføre for å avverge trusler mot personvernet

Hva skal beskyttes?



Oversatt fra en artikkel om DPIA-prosessen: http://friedewald.website/wp-content/uploads/2016/06/apf2016.pdf

Vurdering av personvernkonsekvenser – art. 35

Det er flere typetilfeller der det er nødvendig å utrede personvernkonsekvenser:

- systematisk og omfattende vurdering av personlige forhold når opplysningene brukes til automatiserte avgjørelser
- behandling av sensitive personopplysninger i stort omfang
- systematisk overvåking av offentlig område i stort omfang

I tilfelle man er i tvil anbefaler vi å utføre en DPIA.

Datatilsynet **må** publisere liste over når det er påkrevd.

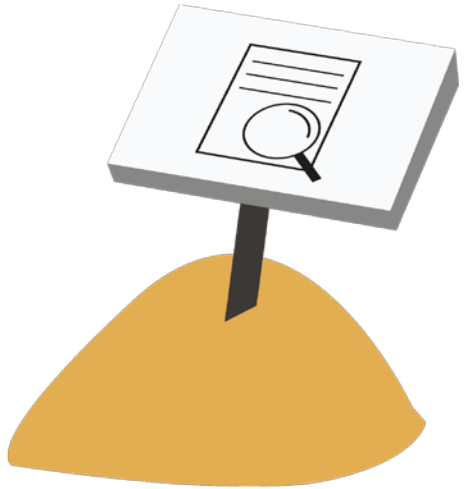
Datatilsynet *kan* publisere liste over når det ikke er påkrevd.

Kriterier

1. Evaluering eller poengvurdering *(scoring)*
2. Automatiserte avgjørelser
3. Systematisk overvåkning (*monitoring*)
4. Sensitive personopplysninger
5. Behandling av personopplysninger i stor skala
6. To eller flere datasett som sammenstilles
7. Personopplysninger om registrerte med særskilt beskyttelsesbehov
8. Ny teknologi eller bruk av eksisterende teknologi til nye formål
9. Konteksten begrenser muligheten for de registrerte til å utøve rettigheter

Forhåndsdrøftelser – Art. 36

- Ved høy risiko, som ikke kan begrenses, skal vi involveres i forhåndsdrøftelser
- Det stilles krav til dokumentasjon som skal sendes inn til oss
- Forordningen stiller krav til vår behandlingstid
- Vi kan veilede eller forby behandlingen



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

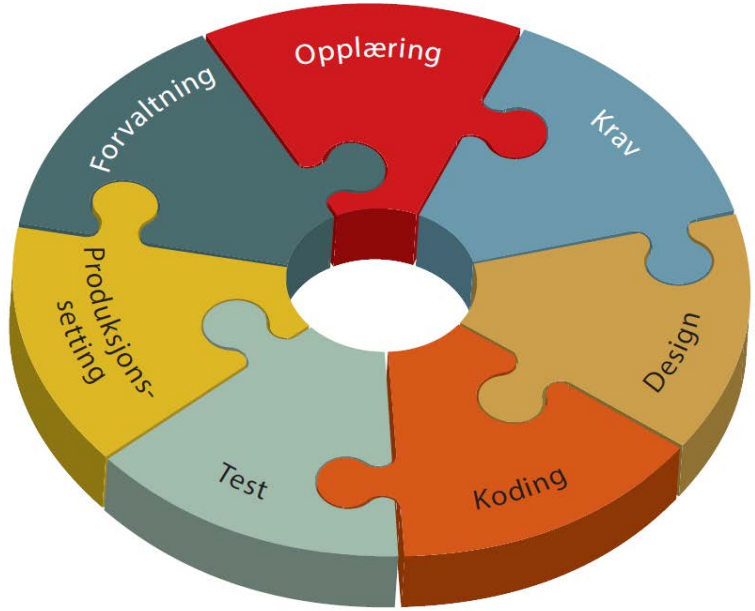
Up to 100 million users downloaded a popular Android app that turned their phones into flashlights. What they didn't realize was that their smartphones also became sophisticated tracking devices, with the app collecting information that could pinpoint their precise location.

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

- Vær i forkant, forebygg fremfor å reparere.
- Gjør personvern til standardinnstilling.
- Bygg personvern inn i designet.
- Skap full funksjonalitet: Både-og, ikke enten-eller.
- Ivareta informasjonssikkerhet fra start til slutt.
- Vis åpenhet.
- Respekter den registrertes personvern.



Oppsummert art 25:

- Obligatorisk
- Tekniske og organisatoriske tiltak.
- Sett det minst personverninngripende alternativet som standard, mht mengde, omfang, lagringstid, tilgjengelighet.
- Ivareta personvernprinsipper og den registrertes rettigheter.


Programvareutvikling med innebygd personvern
Opplæring
Sørg for god kunnskap til regelverk og metodikk tilknyttet programvarens bruksområde ved å:
✓ lage en differensiert opplæringsplan tilpasset ulike profesjoner i utviklingsløpet
✓ forankre opplæringen i ledelsen
Krav
Etabler oversikt over type personopplysninger, behandlingsgrunnlag, formål og ansvarlighet, samt hvem som er behandlingsansvarlig, databehandler og underleverandører. Ivareta personvernprinsipper og de registrertes rettigheter. Sørg for å:
✓ avklare bruk av samtykke eller lovhjemmel for behandlingen
✓ avklare hvilke personopplysninger som er nødvendig for formålet, hvor detaljerte opplysningene må være, om historikk er nødvendig, lagringssted og lagringstid, hvem skal ha tilgang og fra hvor, samt krav til informasjonssikkerhet (bruk for eksempel OWASP ASVS)
✓ vise åpenhet om behandlingen - gi god informasjon om bruk av personopplysninger og hvordan de registrerte kan utøve sine rettigheter
✓ definere toleransenivå
✓ gjennomføre risikovurderinger og vurdering av personvernkonsekvenser
Design
Definer krav til design, analyser angrepsflaten og gjør trusselmodellering. Sørg for:
✓ at den registrertes rettigheter gjenspeiles i programvarens design som er knyttet til personopplysninger og funksjoner, ved å for eksempel begrense og minimere mengden opplysninger, anonymisere eller pseudonymisere, aggregere og sette personvern som standardinnstilling
✓ å analysere hvordan programvaren kan misbrukes ved ulike scenarier og hvordan designet kan forbedres for å unngå identifiserte trusler
Koding
Sørg for sikker koding ved å:
✓ beskrive tillatte verktøy, prosesser og rammeverk for programvareutvikling samt å risikovurdere og godkjenne disse internt i virksomheten
✓ analysere funksjoner, API, tredjepartsbibliotek og moduler - forby de av disse som er utrygge og oppdater de som er utdaterte eller inneholder kjente sårbarheter
✓ regelmessig gjøre statisk kodeanalyse og kodegjennomgang – gjør en automatisk gjennomgang, supplert av manuell for å fange opp svakheter som kan gi feil bruk eller lekkasje av personopplysninger
✓ kontrollere dataflyt, lagring og mellomlagring av personopplysninger
✓ deaktivere unødig sporing, logging og innsamling av personopplysninger
Test
Sikkerhetstesting er en del av testingen. Sørg for å:
✓ teste om personvernkrav og sikkerhetskrav er implementert og riktig implementert
✓ gjennomføre dynamisk testing, fuzz testing og penetrasjonstesting/sårbarhetsanalyse - undersøk om det er kjente sikkerhetsfeil som Cross-site scripting og SQL injection, og test alle input-felt og grensesnitt (bruk for eksempel OWASP Testing Project)
✓ verifisere at angrepsvektorer avdekket i designfasen er håndtert, og at nye angrepsvektorer introdusert under koding er identifisert og håndtert
✓ gjennomgå analysene for trusselmodellering, angrepsflaten, personvernkonsekvenser og sikkerhetsrisiko på nytt for å se at sårbarhetsregulerende tiltak er implementert
✓ bruke fiktive/syntetiske testdata
Produksjonssetting
Programvaren gjøres klar for produksjonssetting ved å:
✓ utarbeide plan for hendelseshåndtering som omfatter håndtering av oppgaver, hendelser, myndighet og roller etter produksjonssetting
✓ gjøre en full sikkerhetsgjennomgang av programvaren, der personvernombud og sikkerhetsrådgiver verifiserer at personvern- og sikkerhetskrav er implementert og fungerer etter hensikten
✓ sørge for at noen med myndighet godkjenner produksjonssetting
✓ arkivere alle vurderinger, analyser, tester, dokumentasjon og kode
Forvaltning
Sørg for å være forberedt på god forvaltning av programvaren ved å:
✓ håndtere hendelser og avvik etter planen
✓ implementere styringssystem for personvern og informasjonssikkerhet som omfatter anskaffelse, forvaltning, drift og vedlikehold, samt rutiner for logging, testing og måling av effekt på organisatoriske og tekniske tiltak
Plakaten oppsummerer Datatilsynets veileder som er basert på artikkel 25 i EUs personvernforordning (GDPR)
Datatilsynet

Innebygd personvern i praksis 2018

Datatilsynet inviterer til konkurranse om beste programvare utviklet utfra prinsippene for innebygd personvern.

Jury:

- Dag Wiese Schartum
- Lillian Røstad
- Maria Bartnes
- Torgeir Waterhouse
- Veronica J. Buer og
  Martha Eike, Datatilsynet

Hvordan delta i konkurransen?

Sende oss et utfylt søknadsskjema med beskrivelse av produktet. Mer informasjon på datatilsynet.no

Frist for innsending av bidrag

1. desember 2017

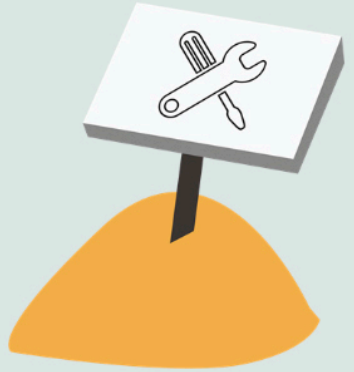
Veilederen ligger på datatilsynet.no

Datatilsynet

Veileder

Programvareutvikling med innebygd personvern

Veilederen skal hjelpe norske virksomheter å forstå og etterleve kravet om innebygd personvern i de nye personvernreglene. Den er utarbeidet i samarbeid med sikkerhetseksperter og programutviklere i privat og offentlig sektor. Veilederen har også vært på høring i flere virksomheter og organisasjoner.



Skriv ut veileder

Innhold

1 Programvareutvikling med innebygd personvern

2 Om veilederen

3 Innebygd personvern - hva er det?

4 Opplæring

5 Krav

Takk for oppmerksomheten!

Datatilsynet

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

datatilsynet.no
personvernbloggen.no

@datatilsynet (Twitter)
@marthaeike