Artificial Intelligence and Data Protection by Design and by Default

Christine Dalebø Gjerdevik | Senior Legal Advisor| Norwegian Data Protection Authority

Data Protection is under pressure

- The World is getting digitalised and personal data is generated and processed at high speed.

- Data protection must be built into the software in order to safeguard data protection in the future.

- The **key persons** for implementing data protection in the digitalised world are those who order and develop software/AI.

Agenda

- GDPR
- Personal data in machine learning
- Principles relating to processing of personal data
  - Including rights and freedoms
- Rights of the data subject
- Data Protection by Design and by Default
  - What does it mean?
  - How to ensure it when developing AI systems?

General Data Protection Regulation

- 25 May 2018
- Applies to all processing of personal data.
- EU/EEA.

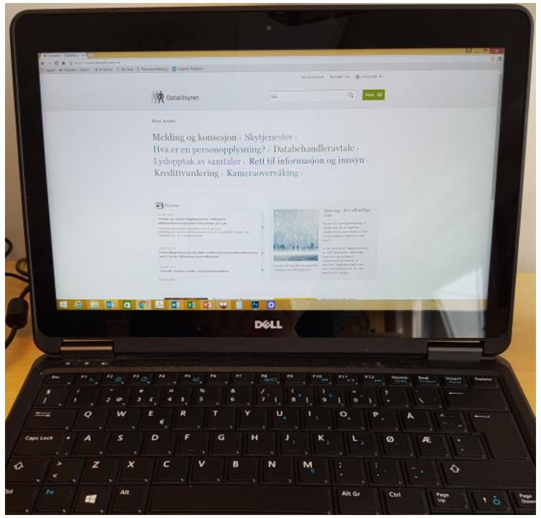
What is personal data?

Any information relating to an identified or identifiable person.

Directly or indirectly.

Peder Aas
2020 Lillevik

F.nr 180262 34997


Datatilsynet
Melding og konsesjon › Skytjenester ›
Hva er en personopplysning? › Databehandleravtale ›
Lydopptak av samtaler › Rett til informasjon og innsyn ›
Kredittvurdering › Kameraovervåking ›
DELL

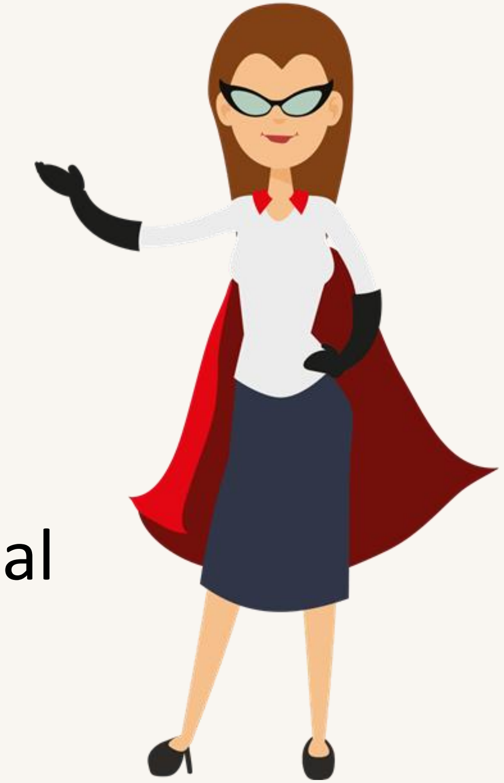
Who is obliged to comply with the GDPR?

Obliged:

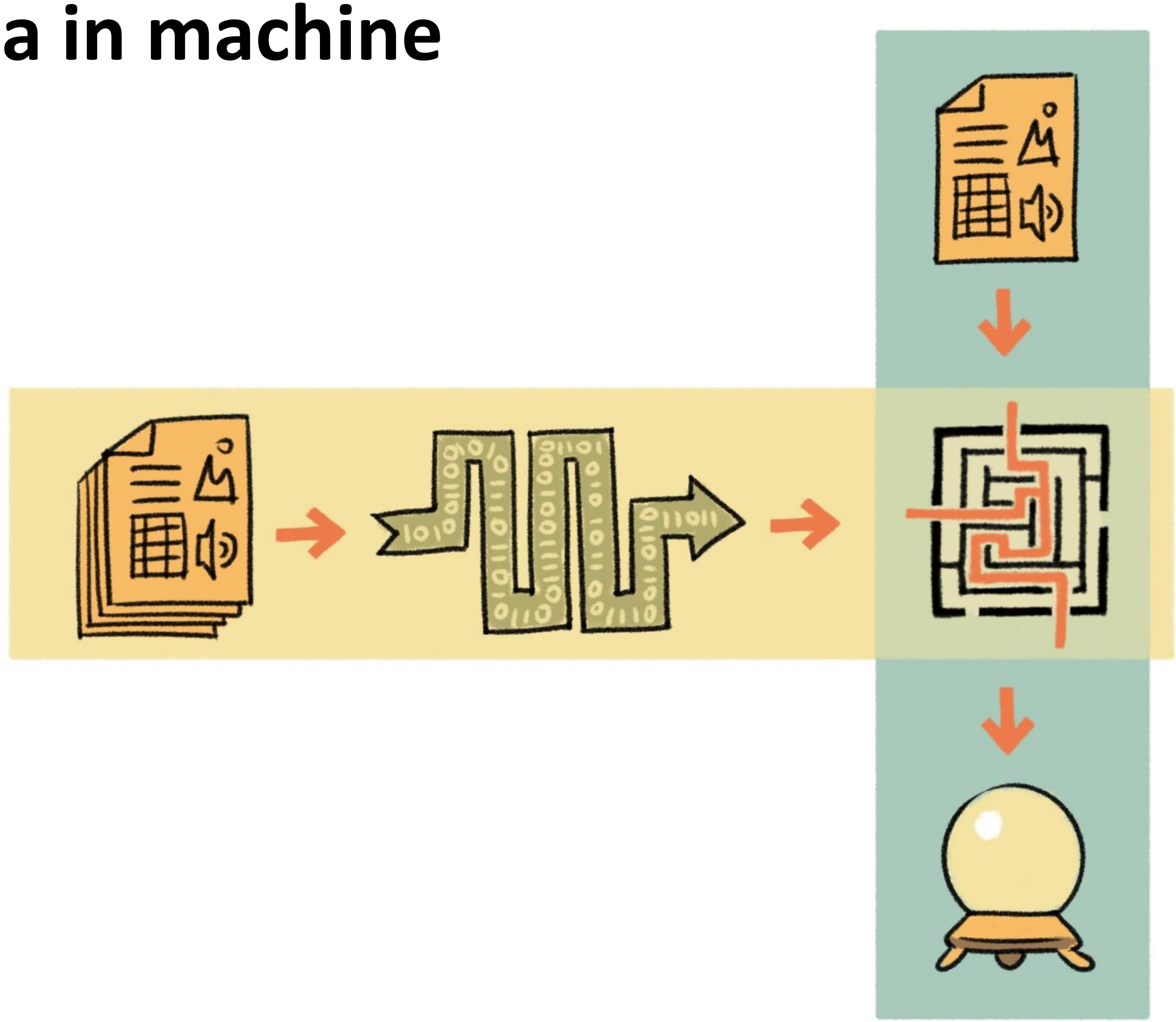
- Controllers
- Processors

Should:

- Companies who develop systems which process personal data



Personal data in machine learning/AI



Principles relating to processing of personal data

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

Article 5 GDPR

Fundamental rights and freedoms and fair processing

- EU Charter for Fundamental Rights and European Convention on Human Rights.

- Such as:
  - Freedom of thought
  - Freedom of expression and information
  - Non-discrimination

- Non-discrimination is especially important with regards to AI.

- Examples: COMPAS and facial recognition systems.

Picture:

Rights of the Data Subject

- Transparent information and communication
- To be given information about the processing of personal data
- Access to the personal data
- Rectification of inaccurate personal data
- Erasure
- Restriction of processing
- Data portability
- Object to further processing of personal data
- Not to be subject to a decision based solely on automated processing

Article 12-22 GDPR

Data Protection by Design and by Default

Data Protection by Design:

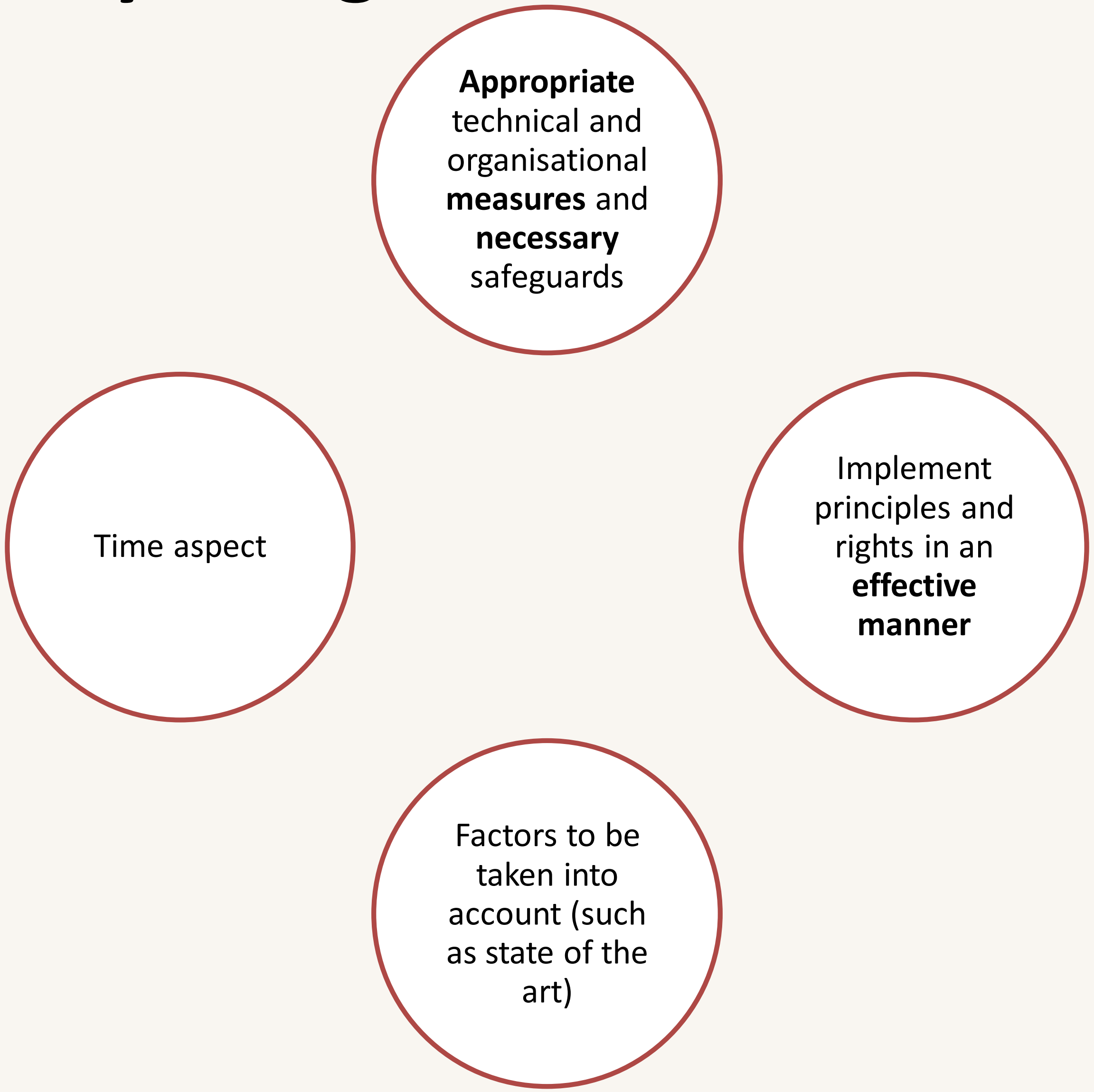
*“Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both **at the time of the determination of the means for processing and at the time of the processing** itself, implement **appropriate technical and organisational measures,** such as pseudonymiation, which are designed to implement data-protection principles, such as data minimisation, in an **effective manner** and to integrate the **necessary safeguards** into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.”*

Data Protection by Default:

*“The controller shall implement **appropriate technical and organisational measures** for ensuring that, by **default**, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*

Article 25 GDPR

Data Protection by Design



Appropriate technical and organisational **measures** and **necessary** safeguards

Time aspect

Implement principles and rights in an **effective manner**

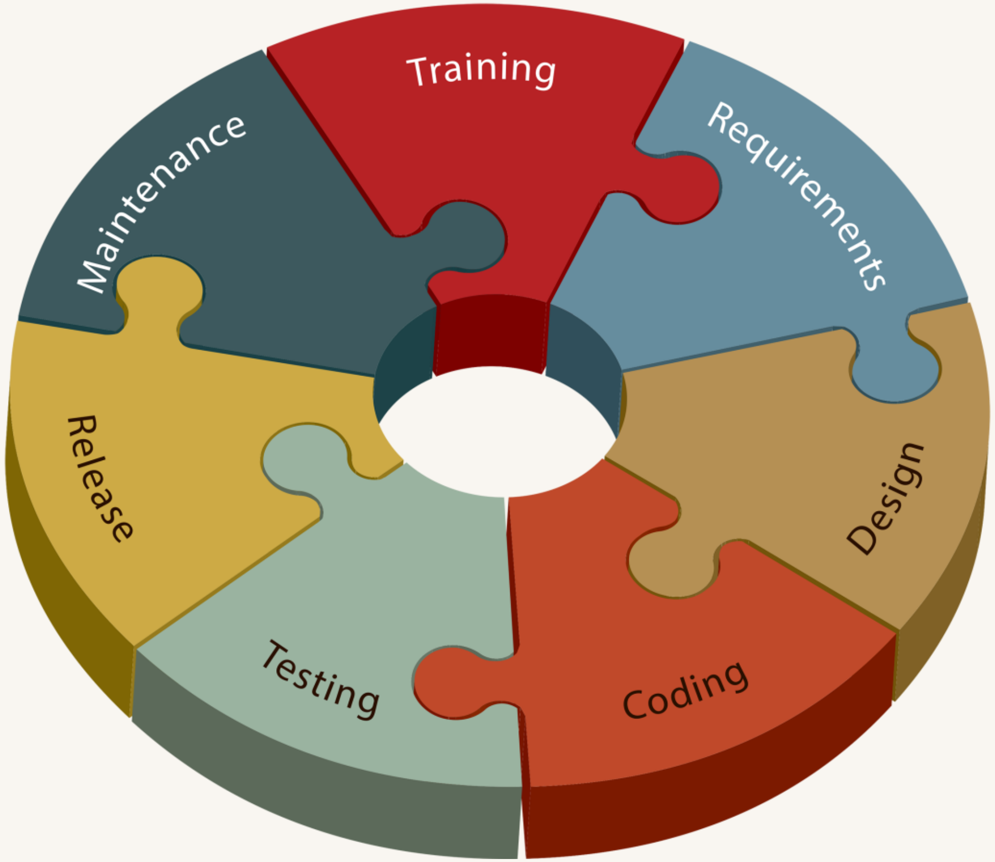
Factors to be taken into account (such as state of the art)

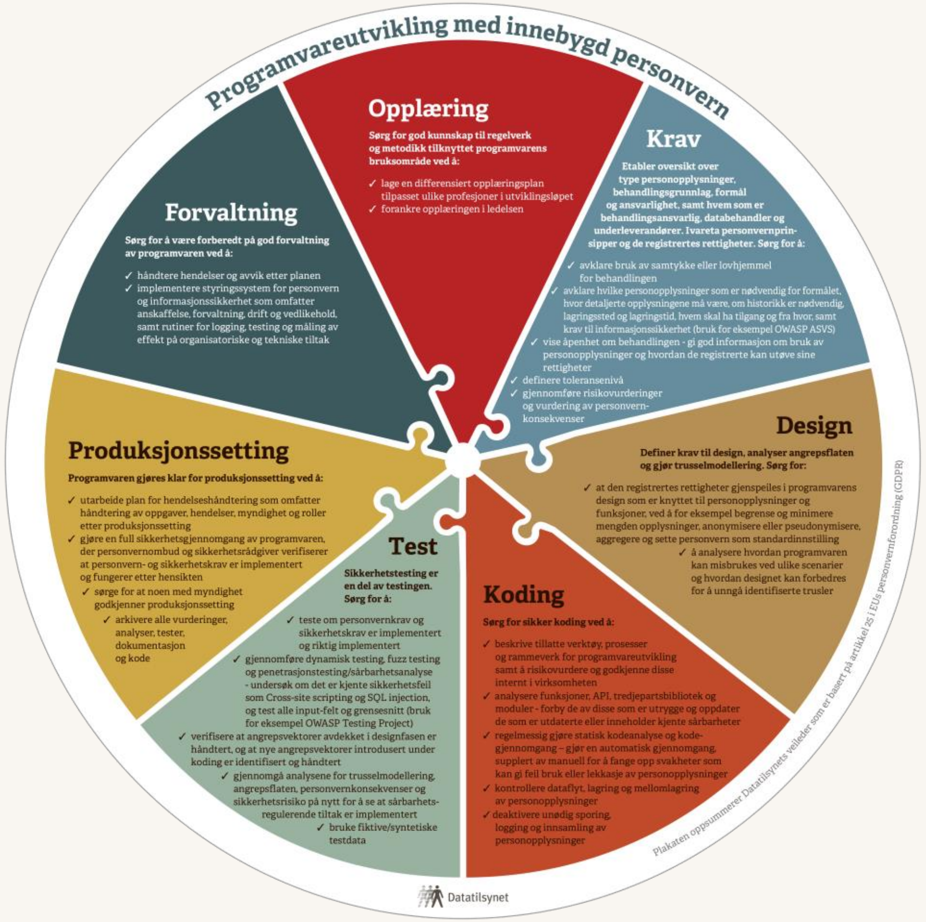
Data Protection by Default

By default

The principles

DPA’s guideline on Data Protection by Design and by Default in software development





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:

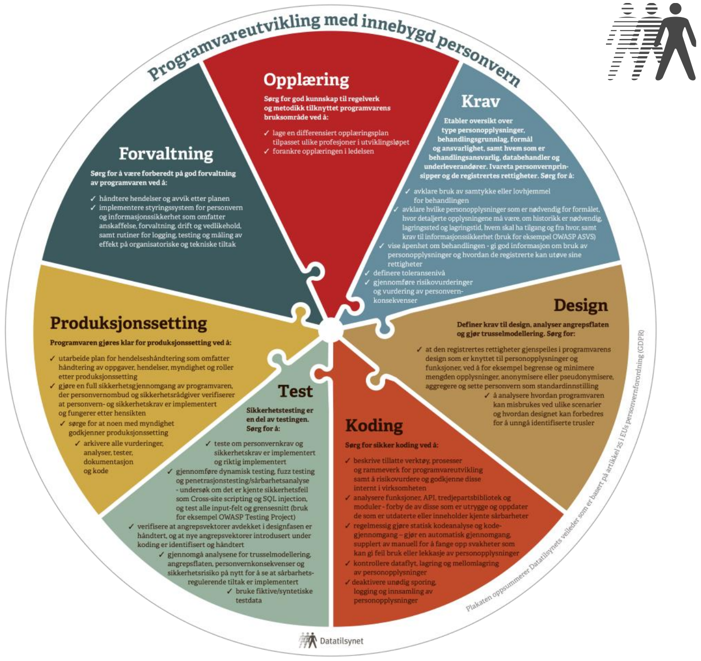
✓ håndtere hendelser og avvik etter planen
✓ implementere styringssystem for personvern og informasjonssikkerhet som omfatter anskaffelse, forvaltning, drift og vedlikehold, samt rutiner for logging, testing og måling av effekt på organisatoriske og tekniske tiltak

Plakaten oppsummerer Datatilsynets veileder som er basert på artikkel 25 i EUs personvernforordning (GDPR)

Datatilsynet

Recommended reading:

- Norwegian DPA’s guide on software development with data protection by design and by default (available in Norwegian and English).
- Norwegian DPA’s report on AI and privacy (available in Norwegian and English).
- EDPB’s guidelines on Automated Decison-Making and Profiling (WP251rev.0.1).
- EDPB guideline on PbDD is in the making.



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 personvern-konsekvenser

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

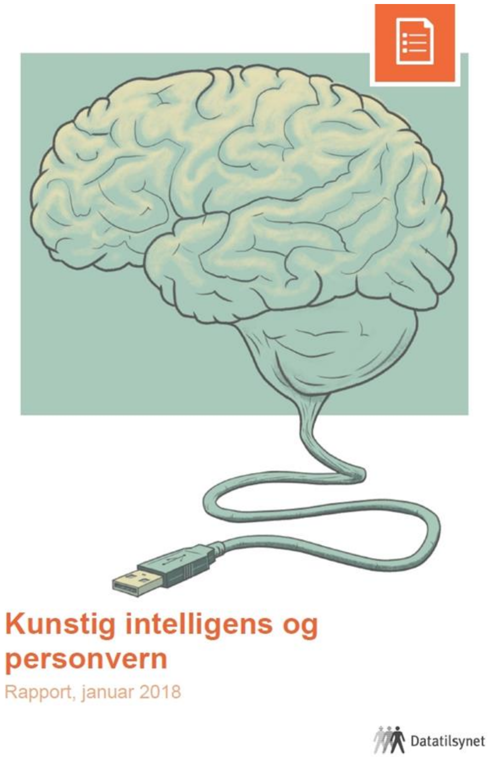
Forvaltning

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



Kunstig intelligens og personvern

Rapport, januar 2018

Datatilsynet

Thank you for your attention

Datatilsynet

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

datatilsynet.no
personvernbloggen.no