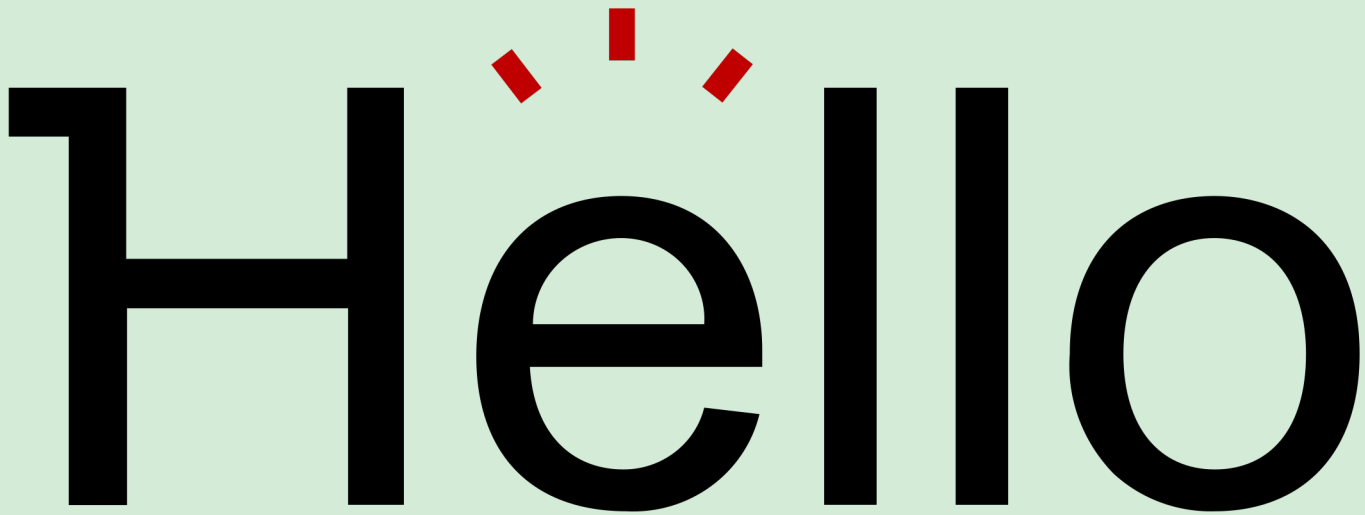

Hëllo

knowit

Privacy by design – ISO 31700

TILT
Oslo 25.05.2023

Andreas Faafeng
Rådgiver informasjonssikkerhet og personvern
Knowit Impact

Introduksjon til Privacy by Design
Introduksjon til ISO 31700

Hvordan personvern?

knowit

Bakgrunn for ISO 31700

Privacy by Design

- The 7 Foundational Principles
- Ann Cavoukian, Ph.D.

GDPR artikkel 25

- Innebygd personvern og personvern som standardinnstilling

ISO 31700

- Privacy by Design for consumer goods and services

Privacy by Design

Ann Cavoukian, Ph.D.

1 Vær i forkant

2 Personvern som standard

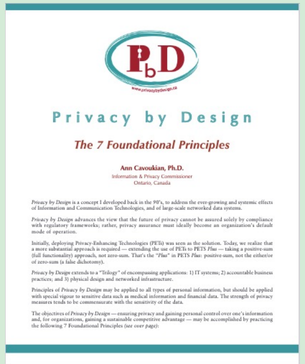
3 Personvern inn i designet

4 Full funksjonalitet

5 Informasjons-sikkerhet

6 Vis åpenhet

7 Vis respekt



www.privacybydesign.ca

Privacy by Design

The 7 Foundational Principles

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

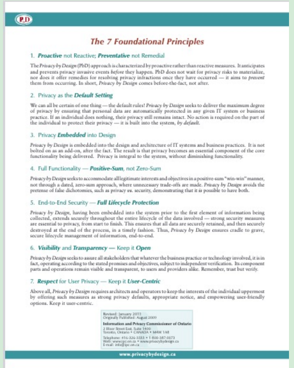
Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:



The 7 Foundational Principles

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial

The *Privacy by Design* (PbD) approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred — it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the ***Default Setting***

We can all be certain of one thing — the default rules! *Privacy by Design* seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy — it is built into the system, *by default*.

3. Privacy ***Embedded*** into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality — ***Positive-Sum***, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy *vs.* security, demonstrating that it is possible to have both.

5. End-to-End Security — ***Full Lifecycle Protection***

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. ***Visibility*** and ***Transparency*** — Keep it ***Open***

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. ***Respect*** for User Privacy — Keep it ***User-Centric***

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

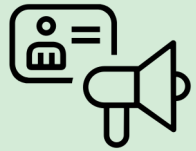
Revised: January 2011
Originally Published: August 2009
Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario • CANADA • M4W 1A8
Telephone: 416-326-3333 • 1-800-387-0073
Web: www.ipc.on.ca • www.privacybydesign.ca
E-mail: info@ipc.on.ca

www.privacybydesign.ca

ISO 31700

Privacy by design for
consumer goods and services

4 Organisering



5 Kommunikasjon

6 Risikohåndtering

7 Bygging

8 Avslutning

Treningssenter

- Treningsenter
- Tilleggstjeneste/abonnement:
  - App som samler brukerens data fra treningsapparater. Data behandles på brukerens enhet og viser informasjon om trening, helse, kosthold mm.
  - Treningssenter inngår samarbeid med leverandør av helse-app.
  - Det stilles krav til at helseopplysninger kun skal lagres i sikker sone på brukeres mobiltelefon med biometrisk autentisering.

ISO 31700:6 – Risikohåndtering

knowit

6.2 Utføre risikovurdering

- ✓ Lag oversikt over personopplysninger
- ✓ Vurder risiko
- ✓ Iverksett tiltak

6.3 Evaluere personvern-risiko hos tredjepart

- ✓ Vurdere tredjeparten
- ✓ Innfør kontrolltiltak

6.4. Dokumentere krav til løsning

- ✓ Formaliser krav til personvern

6.6. Gjør til del av informasjonssikkerhet

- ✓ Inkluder personvern i arbeid med informasjonssikkerhet og beredskap

ISO 31700:5 – Kommunikasjon

knowit

5.3 Deleger ansvar for kommunikasjon

- ✓ Definere rolle
- ✓ Delegerer rolle
- ✓ Oppdater

5.2 Forklar hvordan person-opplysninger behandles

- ✓ Gi kunden god informasjon om hvordan person-opplysninger behandles
- ✓ Gi kunden god informasjon om hvordan kunden selv kan justere behandlingen

5.6 Forberede håndtering av personopplysninger på avveie

- ✓ Definer roller og ansvar
- ✓ Lag kriseplan
- ✓ Øve på krisehåndtering

5.5 Kommuniser til mangfoldig gruppe

- ✓ Språk
- ✓ Alder
- ✓ Teknisk forståelse
- ✓ Kanaler

knowit

ISO 31700

Strukturert planverk for innebygget personvern

Godt tilsvar til GDPR Art.25

Forretningsmuligheter

knowit

Thänks