Bestemmelsen i GDPR art. 25 om innebygd personvern

Emily M. Weitzenböck, Ph.D. (Oslo)
Førsteamanuensis

Seminar – Avdeling for forvaltningsinformatikk,
Universitetet i Oslo
27.02.2019

OSLO METROPOLITAN UNIVERSITY
STORBYUNIVERSITETET

Artikkel 25 nr. 1: Innebygd personvern (DPbDesign)

Art. 25 nr. 1: ‘Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, skal den behandlingsansvarlige, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.’

Artikkel 25 nr. 1: Innebygd personvern (DPbDesign)

Art. 25 nr. 1: ‘Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, skal den behandlingsansvarlige, **både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen**, og **på tidspunktet for selve behandlingen**, gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.’

Artikkel 25 nr. 1: Innebygd personvern (DPbDesign)

Art. 25 nr. 1: ‘Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, skal den behandlingsansvarlige, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, gjennomføre **egnede tekniske og organisatoriske tiltak**, f.eks. pseudonymisering, utformet med sikte på en **effektiv gjennomføring av prinsippene for vern av personopplysninger**, f.eks. dataminimering, og for å **integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter**.’

Artikkel 25 nr. 1: Innebygd personvern (DPbDesign)

Art. 25 nr. 1: ‘**Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører**, skal den behandlingsansvarlige, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.’

Innebygd personvern og personvernprinsippene

Art. 25 nr. 1: ‘Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, **skal den behandlingsansvarlige**, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve behandlingen, **gjennomføre egnede tekniske og organisatoriske tiltak, f.eks. pseudonymisering, utformet med sikte på en effektiv gjennomføring av prinsippene for vern av personopplysninger, f.eks. dataminimering**, og for å integrere de nødvendige garantier i behandlingen for å oppfylle kravene i denne forordning og verne de registrertes rettigheter.’

Innebygd personvern og personvernprinsippene

Art. 25 nr. 1: 'Idet det tas hensyn til den tekniske utviklingen, gjennomføringskostnadene, behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter som behandlingen medfører, **skal den behandlingsansvarlige**, både på tidspunktet for fastsettelse av midlene som skal brukes i forbindelse med behandlingen, og på tidspunktet for selve beha**ndlingen, gjennomføre egnede tekniske og organisatoriske tiltak, som f.eks. pseudonymisering, med sikte på en effektiv gjen**nomføring av dataminimeringsprinsippene, som **personopplysninger, f.e**ksempelvis pseudonymisering, og å integrere nødvendige garantier i be**handlingen for å oppfylle kravene i denne** forordning og verne de re**gistrertes rettigheter.**

Husk: Ikke bare dataminimalitet! Jf. artikkel 5

- ✓ **Lovlighet, rettferdighet og åpenhet**
- ✓ **Formålsbegrensing**
- ✓ **Riktighet**
- ✓ **Lagringsbegrensning**
- ✓ **Integritet og konfidensialitet**
- ✓ **Ansvarlighet**

Artikkel 25 nr. 2: Personvern som standardinnstilling (DPbDefault)

Art. 25 nr. 2: ‘Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles. Nevnte forpliktelse får anvendelse på den mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet. Nevnte tiltak skal særlig sikre at personopplysninger som standard ikke gjøres tilgjengelige for et ubegrenset antall fysiske personer uten den berørte personens medvirkning.’

Artikkel 25 nr. 2: Personvern som standardinnstilling (DPbDefault)

Art. 25 nr. 2: ‘Den behandlingsansvarlige **skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre at det som standard bare er personopplysninger som er nødvendige for hvert spesifikke formål med behandlingen, som behandles**. Nevnte forpliktelse får anvendelse på den mengden personopplysninger som samles inn, omfanget av behandlingen av opplysningene, hvor lenge de lagres og deres tilgjengelighet. Nevnte tiltak skal særlig sikre at personopplysninger som standard ikke gjøres tilgjengelige for et ubegrenset antall fysiske personer uten den berørte personens medvirkning.’

Personvern som standardinnstilling og personvernprinsippene

- Gjennom tekniske og organisatoriske tiltak:
  - Formålsbegrensingsprinsippet
    - nødvendighetskriterium
  - Man skal ha standardinnstillinger for:
    - mengden personopplysninger som samles inn
    - omfang av behandlingen
    - lagringstid
    - tilgjengelighet

Bakgrunn: PbD – The 7 Foundational Principles

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric

Ann Cavoukian

Artikkel 25 nr. 3: Sertifisering

Art. 25 nr. 3: ‘En godkjent sertifiseringsmekanisme i henhold til artikkel 42 kan brukes som en faktor for å påvise at kravene fastsatt i nr. 1 og 2 i denne artikkel overholdes.’

Sml. med andre regulering (1)

- Direktiv 2016/680 om behandling av personopplysninger i politisektoren, Art. 20 – innebygd personvern og personvern som standardinnstilling
- Det gamle PV-direktivet fra 1995:
  - «Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical and organizational measures be taken, **both at the time of the design of the processing system and at the time of the processing itself**, particularly in order to **maintain security and thereby to prevent any unauthorized processing**; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;"

Sml. med andre regulering (2)

- Europarådets (*Council of Europe*) reviderte personvernkonvensjonen 108+: Artikkel 10(3) (*Additional obligations*):

  «3. Each Party shall provide that controllers, and, where applicable, processors, implement technical and organisational measures which take into account the implications of the right to the protection of personal data **at all stages** of the data processing.”

Vage krav: Hva?

- Gjelder alle informasjonssystemer og IT-applikasjoner, både nettbaserte og offline der personopplysninger behandles:
  - spesialutviklet eller tilpasset
  - standard programvare - hyllevare
  - skytjenester
- Gjelder all behandling av personopplysninger:
  - policy/retningslinjer og prosesser i virksomheten må tilrettelegges
  - arbeids- og forvaltningsprosesser

Vage krav: Hva?

- Nye systemer:
  - Gjelder ved «utvikling, utforming, valg og bruk av programmer, tjenester og produkter», fortalepunkt 78
  - Forordningen: Art. 25; Art. 35: utrede personvernkonsekvensene (DPIA) vedr. planlagt behandling av personopplysninger som sannsynligvis vil utgjøre høy risiko for personers rettigheter, herunder hvilke ***tiltak*** som skal settes i verk.
- Eksisterende systemer?
  - PV-forordningen gjør ikke unntak for eldre IT-systemer
    - Utgangspunkt: ja!
    - Avveining: risiki for de registrerte vs. kostnader
    - Tenk alternativt!

Risikobasert tilnærming

- “The Working Party recognizes that some of the provisions in the proposed Regulation may pose a burden on some controllers which may be perceived as unbalanced and has therefore ... already expressed the view that **all obligations must be scalable to the controller and the processing operations concerned**. […] Data subjects should have the same level of protection, regardless of the size of the organisation or the amount of data it processes. Therefore the Working Party feels that all controllers must act in compliance with the law, though this can be done on in a **scalable** manner.”
- "Implementation of controllers’ obligations through accountability tools and measures (e.g. impact assessment, **data protection by design**, data breach notification, security measures, certifications) **can and should be varied according to the type of processing and the privacy risks for data subjects**. There should be recognition that not every accountability obligation is necessary in every case – for example where processing is small-scale, simple and low-risk."

Statement on the role of a risk-based approach in data protection legal frameworks (WP218)

Vage krav: Hvem?

- **BA:**
  - Artikkel 25
- **DB:**
  - Implisitt, jf. art. 28(1) men denne forpliktelsen påhviler BA
- **Utviklere?**
  - Fortalepunkt 78: “**oppmuntres til å ta hensyn til**"
  - EDPS uttalelse, avsnitt 182: "The principles of data protection by design and by default are not presently addressed to advisers, developers and producers of hardware or software. **However, they will be relevant for them from the start, as controllers are bound by them and accountable for compliance. In other words, obligations for controllers** (and for processors, as mentioned above) **are likely to create some incentives for the market of relevant goods and services**."

Mekanismer: Sertifisering

Art. 25(3): "En godkjent sertifiseringsmekanisme i henhold til artikkel 42 kan brukes som en faktor for å påvise at kravene fastsatt i nr. 1 og 2 i denne artikkel overholdes."

- Sertifiseringsmerke fra en akkreditert organisasjon, jf. art. 43.
- Frivillig ordning
- Fritar ikke BA fra kravene i forordningen
- EDPB Guidelines 4/2018 on the accreditation of certification bodies under Article 43 of the GDPR

Sertifiseringsmerker - eksempler

Innebygd personvern: Eksempler

1. Unngå unødvendig innsamling av personopplysninger, f.eks. nettbasert skjema med svar som velges fra en nedtrekksliste istedenfor fritekst.
2. Lagringstid, f.eks. mulig å datomerke informasjon med utløpsdato; hvis juridisk mulig, implementere automatiserte slette- eller arkivrutiner; varsel om at en bør vurdere å overføre opplysninger til arkiv.
3. Tilgangsstyring
4. e-Resept ordningen

Innebygd personvern – ikke bare å ivareta informasjonssikkerhet

- **Informasjonssikkerhet:**
  - *(Personverndirektivet), Forordning:*
    - konfidensialitet
    - integritet
    - tilgjengelighet
  - ISO/IEC 27001 (Krav til informasjonssikkerhet) og 27000-serie
- **Innebygd personvern og personvern som standardinnstilling** – tekniske og organisatoriske tiltak som:
  - Ivaretar informasjonssikkerhet fra start til slutt
  - **Ivaretar personvernprinsippene, slik som dataminimalitet**
  - **Verne de registrertes rettigheter, herunder legge til rette for informerte registrerte / brukermedvirkning**
    - Gjennomsiktighet
    - kontroll
  - jf. fortalens avsnitt 78

Eight Privacy Design Strategies: Hoepman

1. **MINIMISE**: The amount of personal information that is processed should be minimal.
2. **HIDE**: Any personal information that is processed should be hidden from plain view.
3. **SEPARATE**: Processing should be done in a distributed fashion whenever possible.
4. **AGGREGATE**: Processing only at highest level of aggregation and least possible detail.
5. **INFORM**: Data subjects should be adequately informed.
6. **CONTROL**: Right to view, update, and ask for deletion of personal data collected.
7. **ENFORCE**: Have in place and enforce a privacy policy compatible with legal req.
8. **DEMONSTRATE**: Be able to demonstrate compliance.

"Privacy design strategies", J.-H. Hoepman, Proceedings of the 29th IFIP TC 11 International Conference, 2014, 446-459

WhatsApp

WHATSAPP WEB EGENSKAPER LAST NED SIKKERHET FAQ

How do I choose not to share my account information with Facebook to improve my Facebook ads and products experiences?

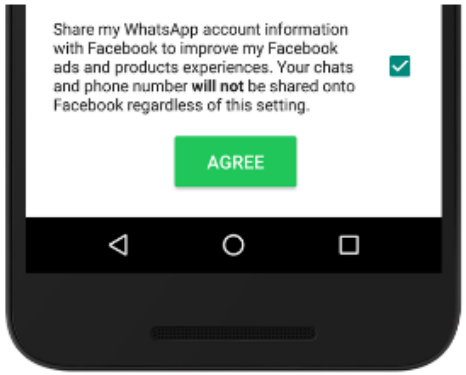
If you are an existing user, you can choose not to share your account information with Facebook to improve your Facebook ads and products experiences.

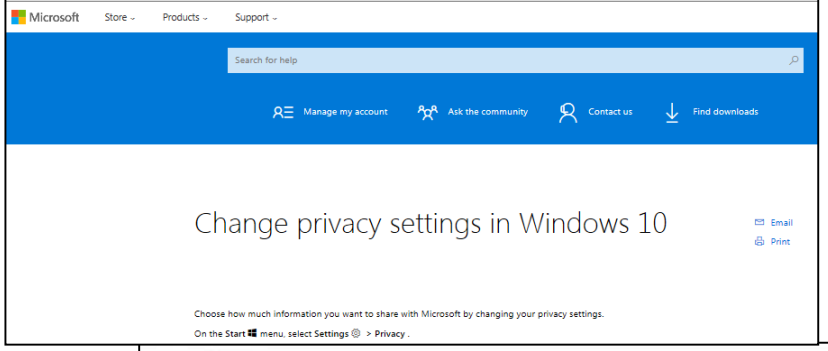
There are two ways to do this:

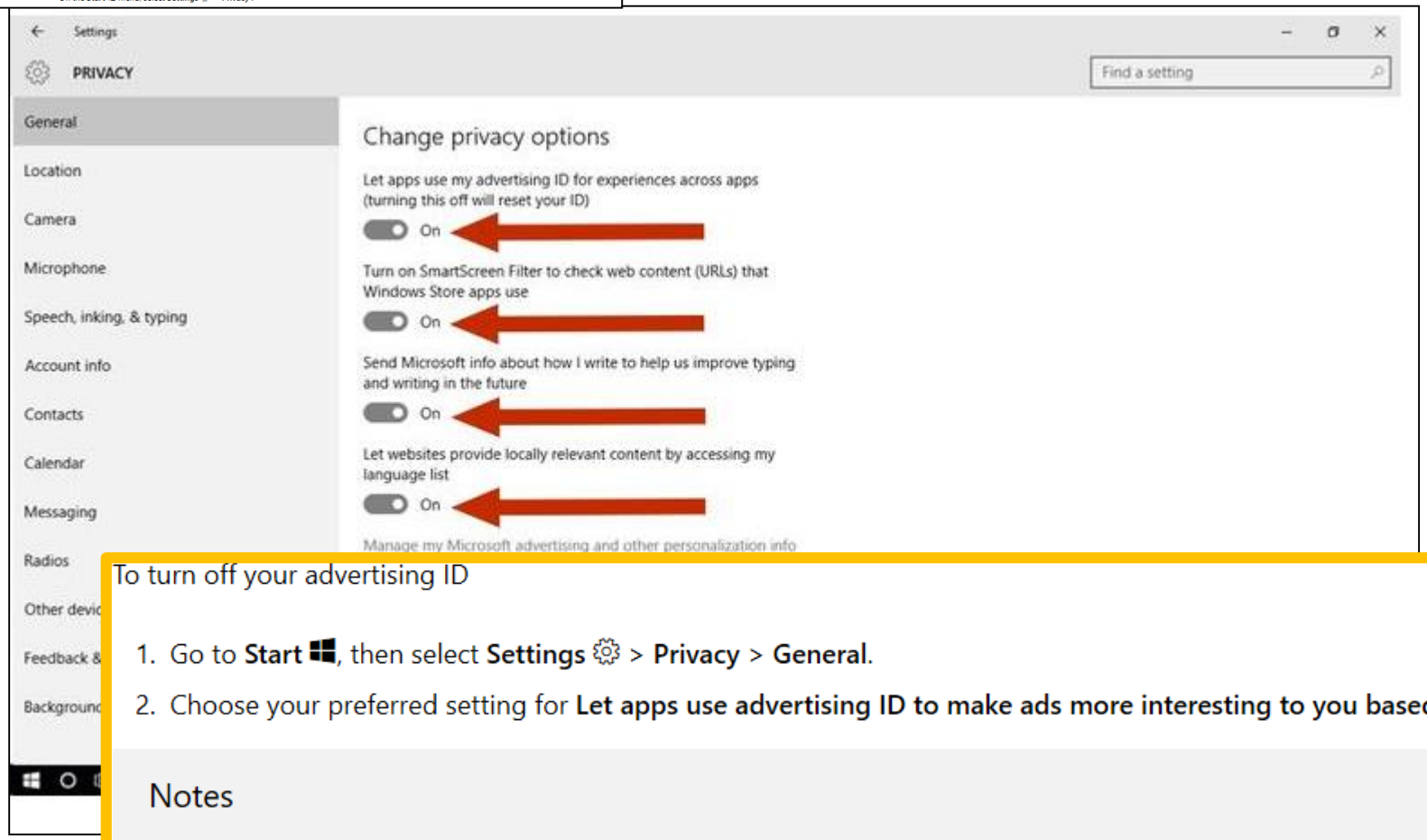
Option 1

Before you tap **Agree** to accept our updated Terms of Service and Privacy Policy, tap **Read**.

You will see a control at the bottom of the screen. If you do not want your account information shared with Facebook to improve your Facebook ads and products experiences, you can uncheck the box or toggle the control.







To turn off your advertising ID

1. Go to **Start**, then select **Settings** > **Privacy** > **General**.
2. Choose your preferred setting for **Let apps use advertising ID to make ads more interesting to you based on your app activity**.

Notes

- Turning the advertising ID off will not reduce the number of ads you see, but it may mean that ads are less interesting and relevant to you. Turning it back on will reset the advertising ID.
- In previous versions of Windows 10, advertising ID was referred to as relevant ads.

Opt out of seeing personalised ads

You can opt out of personalised ads in your Ads Settings. Your opt outs will apply across both Google ads services (ex: Search ads) and the 2+ million websites and apps that partner with Google to show ads.

Instructions

Ads Settings lets you opt out of seeing personalised ads when you're:

- Signed in to your Google Account ("Ads Personalisation")
- Signed out of your Google Account and browsing the websites and apps that partner with Google to show ads ("Ads Personalisation Across the Web")
- Signed out of your Google Account and using Google Search ("Ads Personalisation on Google Search")

If you're signed in to your Google Account

If you're signed out of your Google Account

If you want to turn off ads personalisation for your browser

Opt out of seeing personalised ads

You can opt out of personalised ads in your Ads Settings. Your opt outs will apply across both Google ads services (ex: Search ads) and the 2+ million websites and apps that partner with Google to show ads.

Instructions

Ads Settings lets you opt out of

- Signed in to your Google Acc
- Signed out of your Google Ac
  ("Ads Personalisation Across
- Signed out of your Google Ac

If you're signed in to your

If you're signed out of you

If you want to turn off ads

What opting out doesn't do

There are some things that opting out doesn't do. Here are some of the most common scenarios and what you can do to address them.

- Stop ads altogether
- Disable other companies' personalised ads
- Opt you out across multiple browsers or computers at once if you're signed out of your Google Account
- Keep you opted out after you've cleared your browser cookies
- Keep you opted out if your browser blocks cookies
- Opt you out of personalised ads in services where cookie technology may not be available

Takk for meg!

emmawe@oslomet.no