Førsteamanuensis Emily M. Weitzenboeck

Krav til konsekvensvurdering og forhåndsdrøfting

Personvernkonferansen 2017
Hotell Bristol, Oslo

Emily-Mary.Weitzenboeck@hioa.no

Disposisjon

- Krav til konsekvensvurdering, jf. artikkel 35
  - Innhold
  - Når inntrer plikten
- Krav til forhåndsdrøfting, jf. artikkel 36
  - Hva er det og når må man forhåndsdrøfte?

HØGSKOLEN I OSLO
OG AKERSHUS

Hva er en vurdering av personvernkonsekvenser?

"A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them."

Artikkel 29-Gruppen

HØGSKOLEN I OSLO
OG AKERSHUS

Hva er en vurdering av personvernkonsekvenser?

"A DPIA is a process designed to describe the processing, assess its necessity and proportionality and help manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining the measures to address them."

"[…] a DPIA is a process for building and demonstrating compliance."

Artikkel 29-Gruppen

HØGSKOLEN I OSLO OG AKERSHUS

Krav til vurdering av personvernkonsekvenser (DPIA)

- Der behandlingen trolig vil resultere i stor risiko til individets rettigheter og friheter, plikter BA å gjennomføre en vurdering av personvernkonsekvensene (DPIA), jf. art. 35 nr. 1:
  - "trolig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet."

HØGSKOLEN I OSLO OG AKERSHUS

«fysiske personers rettigheter og friheter»: WP 218

- Artikkel 29-Gruppen: *Statement on the role of a risk-based approach in data protection legal frameworks*, WP 218, 30.5.2014:
  - "8/ In the context referred to above [art. 35], the scope of "the rights and freedoms" of the data subjects primarily concerns the right to privacy but may also involve other ***fundamental*** rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion." (vår utheving)
  - Merk ordlyd i art. 35 nr. 1: "fysiske personers rettigheter og friheter" …

HØGSKOLEN I OSLO OG AKERSHUS

«fysiske personers rettigheter og friheter»: Tidligere utkast av artikkel 35 nr. 1

- **Tidligere utkast av artikkel 35 nr. 1 (Rådets forslag):**
  - *"*Where *a type of* processing *in particular using new technologies, and taking into account the* nature, *scope, context and* purposes *of the processing, is likely to result in a high risk for the rights and freedoms of individuals,* ***such as discrimination, identity theft or fraud, financial loss, damage to the reputation, unauthorised reversal of pseudonymisation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage***, the controller shall*, prior to the processing,* carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*"* (vår utheving)
- **Inntatt i fortalens nr. 75:**
  - *"*når behandlingen kan føre til forskjellsbehandling, identitetstyveri eller -bedrageri, økonomisk tap, skade på omdømme, tap av fortrolighet for taushetsbelagte personopplysninger, uautorisert oppheving av pseudonymisering eller andre betydelige økonomiske eller sosiale ulemper*"*

HØGSKOLEN I OSLO OG AKERSHUS

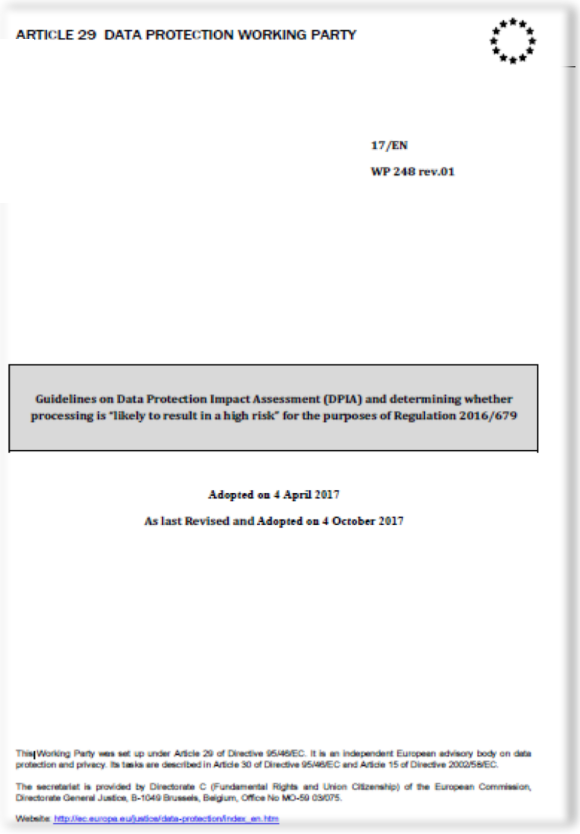
Tilfeller der DPIA er alltid nødvendig (art. 35 nr. 3):

- Systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for den fysiske personen eller på lignende måte i betydelig grad påvirker den fysiske personen
- Behandling i stor skala av sensitive personopplysninger eller opplysninger om straffedommer og straffbare forhold
- Systematisk overvåking i stor skala av et offentlig tilgjengelig område

HØGSKOLEN I OSLO
OG AKERSHUS

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

Artikkel 29-Gruppen, WP 248 rev.01 (4.10.2017)



ARTICLE 29 DATA PROTECTION WORKING PARTY

17/EN
WP 248 rev.01

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679

Adopted on 4 April 2017

As last Revised and Adopted on 4 October 2017

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 03/075.

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

HØGSKOLEN I OSLO
OG AKERSHUS

Kriterier for å avgjøre om det trolig vil medføre høy risiko, jf. Artikkel 29-Gruppen, WP 248 rev.01

1. Evaluation or scoring, including profiling and predicting, especially from "*aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements" (jf. fortalens nr. 75)*
2. Automated-decision making with legal or similar significant effect (jf. art. 35 nr. 3 bokstav a)
3. Systematic monitoring: processing used to observe, monitor or control data subjects, including data collected through networks or "*a systematic monitoring of a publicly accessible area*", (jf. art. 35 nr. 3 bokstav c)
4. Sensitive data or data of a highly personal nature
5. Data processed on a large scale

HØGSKOLEN I OSLO OG AKERSHUS

Kriterier for å avgjøre om behandling krever DPIA, jf. Artikkel 29-Gruppen, WP 248 rev.01

6. Matching or combining datasets
7. Data concerning vulnerable data subjects
8. Innovative use or applying new technological or organisational solutions
9. When the processing in itself *"prevents data subjects from exercising a right or using a service or a contract"* (Article 22 and recital 91).

Hvis minst ***to*** av disse er aktuelle, er det sannsynlig at DPIA må gjøres.

Kan være nødvendig også om ***ett*** kriterium er oppfylt.

HØGSKOLEN I OSLO OG AKERSHUS

Andre momenter i art. 35 nr. 1:

- "trolig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet."
- "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))

HØGSKOLEN I OSLO OG AKERSHUS

Unntak fra plikten til DPIA

- Dersom behandling iht art. 6 nr. 1 bokstav c eller e har et rettslig grunnlag i EU eller nasjonal lov, og det allerede er utført en vurdering av personvernkonskvenser som en del av en generell konsekvensvurdering ifm vedtakelse av nevnte rettslige grunnlag, jf. Art. 37 nr. 10.
- Kan fastsettes I nasjonal rett at det likevel skal gjøres en DPIA – Justisdepartementet foreslår ingen generell regel om konsekvensutredning i disse tilfeller.

HØGSKOLEN I OSLO OG AKERSHUS

Ja/nei lister

- Datatilsynet **skal** utarbeide og offentliggjøre en liste over hvilke type behandlingsaktiviteter som krever DPIA, jf. Art. 35 nr. 4
- Datatilsynet **kan** utarbeide og offentliggjøre en liste over hvilke typer behandlingsaktiviteter som ikke krever DPIA, jf. art. 35 nr. 5
- Listene oversendes til EDPB (Personvernrådet):
  - Konsistensmekanisme, jf. art. 35 nr. 6, jf. art. 64.

HØGSKOLEN I OSLO OG AKERSHUS

Hvem?

- **Behandlingsansvarlig:**
  - "Dersom det er trolig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal **den behandlingsansvarlige** før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet. En vurdering kan omfatte flere lignende behandlingsaktiviteter som innebærer tilsvarende høye risikoer."
  - BAs plikt til å **rådføre seg med personvernombudet**, dersom en slik er utpekt, ifm utførelsen av DPIA, jf. art. 35 nr. 2.
- **Databehandleren?** Se fortalens nr. 95:
  - "Databehandleren bør ved behov og på anmodning bistå den behandlingsansvarlige med å overholde pliktene som er forbundet med utførelsen av vurderingen av personvernkonsekvenser, og med forhåndsdrøftinger med tilsynsmyndigheten."

HØGSKOLEN I OSLO OG AKERSHUS

Beskjeden rolle for de registrerte

"Dersom det er relevant, skal den behandlingsansvarlige innhente synspunkter på den planlagte behandlingen fra de registrerte eller deres representanter uten at det berører vernet av kommersielle eller allmenne interesser eller sikkerheten ved behandlingsaktivitetene.", jf. art. 35 nr. 9

HØGSKOLEN I OSLO OG AKERSHUS

På hvilket tidspunkt skal en DPIA foretas?

- "Før behandlingen", jf. art. 35 nr. 1
  - I overenstemmelse med prinsippet om innebygd personvern og personvern som standardinnstilling (art. 25)
  - Bør settes i gang så tidlig som mulig i utformingen av behandlingsaktiviteter
  - Ajourføring av vurderingen gjennom prosjektets levetid
- Hva med allerede eksisterende behandlingsaktiviteter?
  - Ikke nødvendig for behandlingsaktiviteter som har allerede fått konsesjon fra Datatilsynet, og som gjennomføres på en måte som ikke er endret siden den forutgående kontrollen, jf. overgangsregelen i fortalens nr. 171.
  - Dersom det har vært en endring i gjennomføringsbetingelser (omfang, formål, innsamlet personopplysninger, osv.) som trolig medfører en høy risiko ELLER dersom det har vært en endring av risiki ➡ DPIA

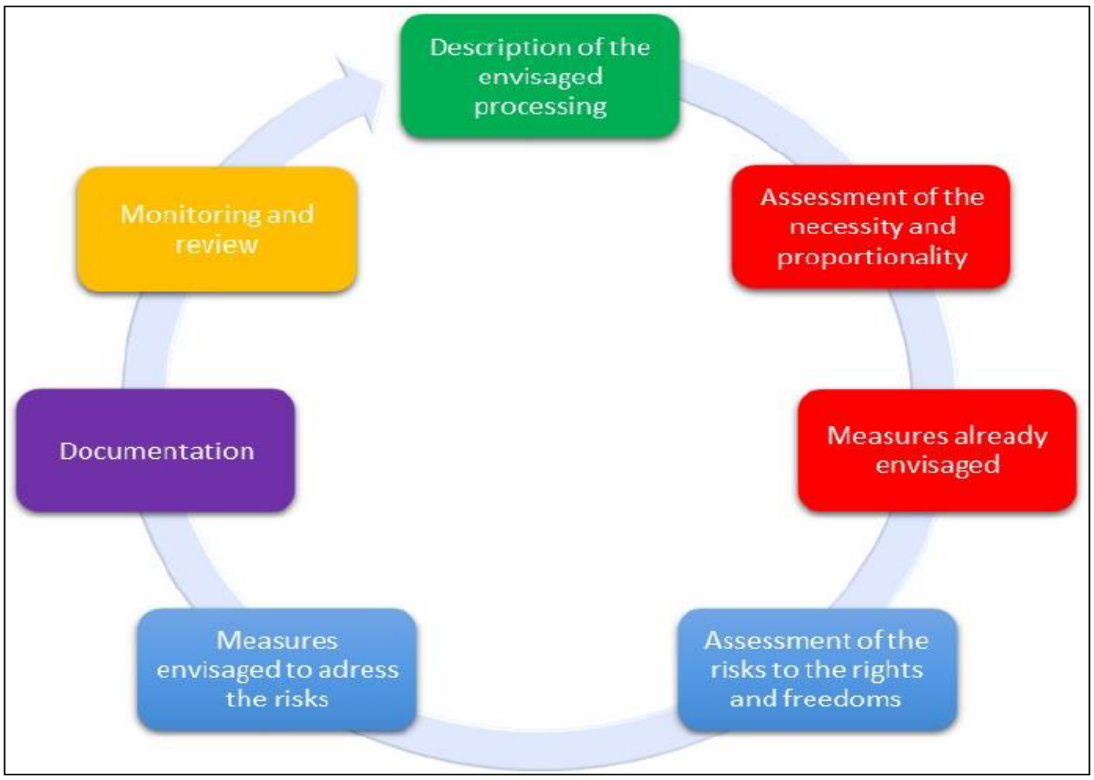
HØGSKOLEN I OSLO OG AKERSHUS

Krav til innholdet i DPIA, jf. art. 35 nr. 7

a) "en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen, herunder, dersom det er relevant, den berettigede interessen som forfølges av den behandlingsansvarlige,
b) en vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene,
c) en vurdering av risikoene for de registrertes rettigheter og friheter som nevnt i nr. 1, og
d) de planlagte tiltakene for å håndtere risikoene, herunder garantier, sikkerhetstiltak og mekanismer for å sikre vern av personopplysninger og for å påvise at denne forordning overholdes, idet det tas hensyn til de registrertes og andre berørte personers rettigheter og berettigede interesser"

HØGSKOLEN I OSLO OG AKERSHUS

Prosessen for å utføre DPIA, jf. WP 248 rev.01



HØGSKOLEN I OSLO OG AKERSHUS

Kontroll og revisjon

- "Ved behov skal den behandlingsansvarlige foreta en gjennomgåelse for å vurdere om behandlingen utføres i samsvar med vurderingen av personvernkonsekvenser, i det minste dersom risikoen som behandlingen medfører, endres." jf. artikkel 35 nr. 11.
- Formulering foreslått av Europa Parlement hadde tydelig krav om at dette skal skje minst hver 2 år.

HØGSKOLEN I OSLO OG AKERSHUS

Risikovurdering etter POL/POF v. DPIA

- Risikovurderinger skal alltid foretas som en del av internkontroll, jf. POL § 13 og POF § 2-4.
  - Fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger
  - Klarlegge sannsynligheten for og konsekvenser *for virksomheten* av sikkerhetsbrudd (brudd av konfidensialitet, integritet og tilgjengelighet).
- DPIA etter Personvernforordningen ser på hva konsekvenser er *for de registrerte*.

HØGSKOLEN I OSLO OG AKERSHUS

F. Bieker et al (2016)

Fig. 2. Protection Goals

"Unlinkability ensures data cannot be linked across different domains and/or be used for purposes differing from the original intent. Transparency means that the data subjects have knowledge of all relevant circumstances and factors regarding the processing of their personal data. Lastly, intervenability entails the control of the data subjects, as well as the controller or supervisory authority over the personal data."

HØGSKOLEN I OSLO OG AKERSHUS

Risikostyring v. Krav til vurdering av personvernkonsekvenser

- Begge gjelder identifisering og evaluering av risiki
- "The latter [risk management] usually addresses risks for an organization and its activities. This is not the case in Article 35(1) GDPR, which concerns the risk for the rights and freedoms of individuals. Thus, unlike in risk management, there is no acceptable residual risk and every processing of personal data is an interference with the individual rights and freedoms and has to be justified."

(F. Bieker et al (2016) s. 24)

HØGSKOLEN I OSLO OG AKERSHUS

DPIA som «metaregulering»

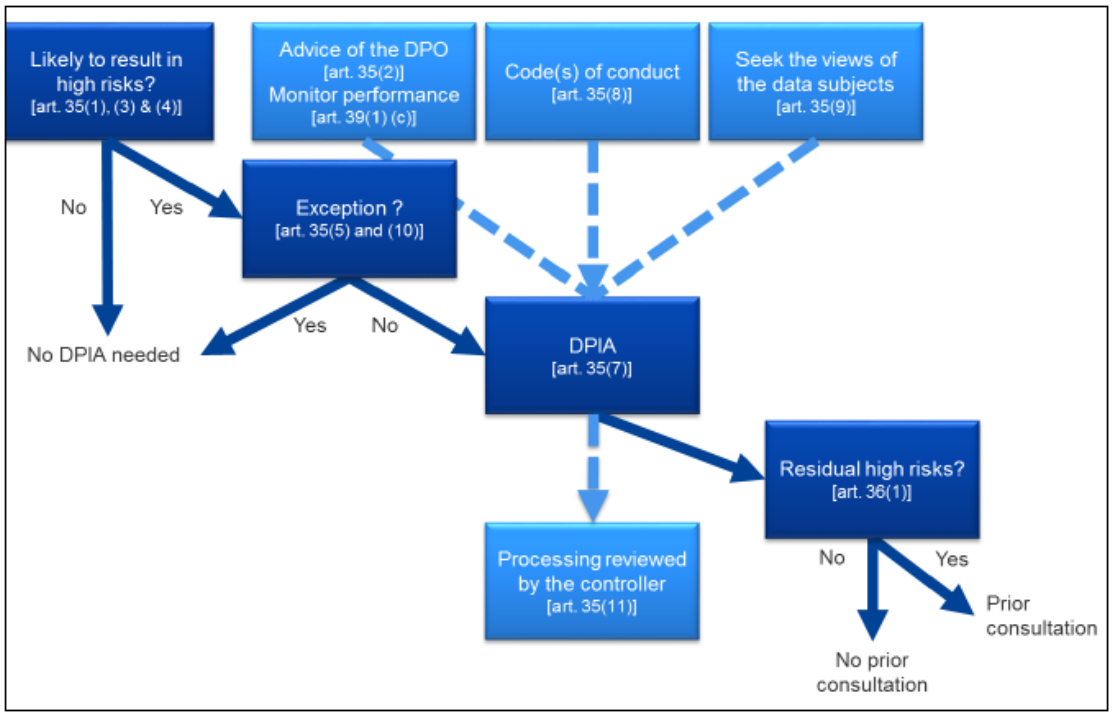
- Fra et selvreguleringsverktøy til et obligatorisk verktøy for visse typer behandlinger av personopplysninger, jf. art. 35.
- R. Binns (2017) beskriver DPIA som *meta-regulation* (Parker):
  - "Mandatory impact assessments differ from traditional prescriptive legal regulation; they are a combination of rules prescribed by the regulator, and policies that the regulatees must devise for themselves and impose upon themselves (with input from stakeholders)." (Binns, s. 29).

HØGSKOLEN I OSLO OG AKERSHUS

Når skal det foretas forhåndsdrøftinger?

- Dersom en vurdering av personvernkonsekvenser foretatt iht artikkel 35 viser at behandlingen vil medføre en høy risiko i mangel av tiltak truffet av den behandlingsansvarlige for å begrense risikoen, skal den behandlingsansvarlige rådføre seg med Datatilsynet før behandlingen.
  - Engelsk versjon: "[…] would result in a high risk in the absence of measures taken by the controller to mitigate the risk."
- "When residual risks are high", *Guidelines*, s. 18

HØGSKOLEN I OSLO OG AKERSHUS



Guidelines, s. 7

HØGSKOLEN I OSLO OG AKERSHUS

Dokumentasjon som skal framlegges DT

- Dersom det er relevant, ansvarsfordelingen mellom den behandlingsansvarlige, de felles behandlingsansvarlige og databehandlerne som er involvert i behandlingen, særlig ved behandling i et konsern,
- Formålene med og midlene for den planlagte behandlingen
- Tiltakene og garantiene som er fastsatt for å verne de registrertes rettigheter og friheter i henhold til personvernforordningen
- Dersom det er relevant, kontaktopplysningene til personvernombudet
- Vurderingen av personvernkonsekvenser fastsatt i artikkel 35, og
- All annen informasjon som tilsynsmyndigheten anmoder om.

(jf. artikkel 36 nr. 3]

HØGSKOLEN I OSLO OG AKERSHUS

Datatilsynets rolle

- Gi skriftlige råd til den behandlingsansvarlige og, dersom det er relevant, databehandleren, OG
- Kan bruke andre virkemidler, jf. Artikkel 58:
  - Undersøkelsesmyndighet
  - Korrigerende tiltak
  - Myndighet til å godkjenne og gi råd

HØGSKOLEN I OSLO OG AKERSHUS

Tidsfrister

- Skriftlige råd innen 8 uker fra mottak av anmodningen om drøftinger
- Kan forlenges med 6 uker, når behandlingen er kompleks (artikkel 36 nr. 2)
  - DT skal underretter den behandlingsansvarlige (evt. databehandleren) om årsakene til forlengelse senest en måned etter å ha mottatt anmodninger om drøftinger.
  - Tidsfrister kan utsettes midlertid til DT har innhentet informasjonen den har anmodet ifm drøftingene.

HØGSKOLEN I OSLO OG AKERSHUS

Høringsnotat

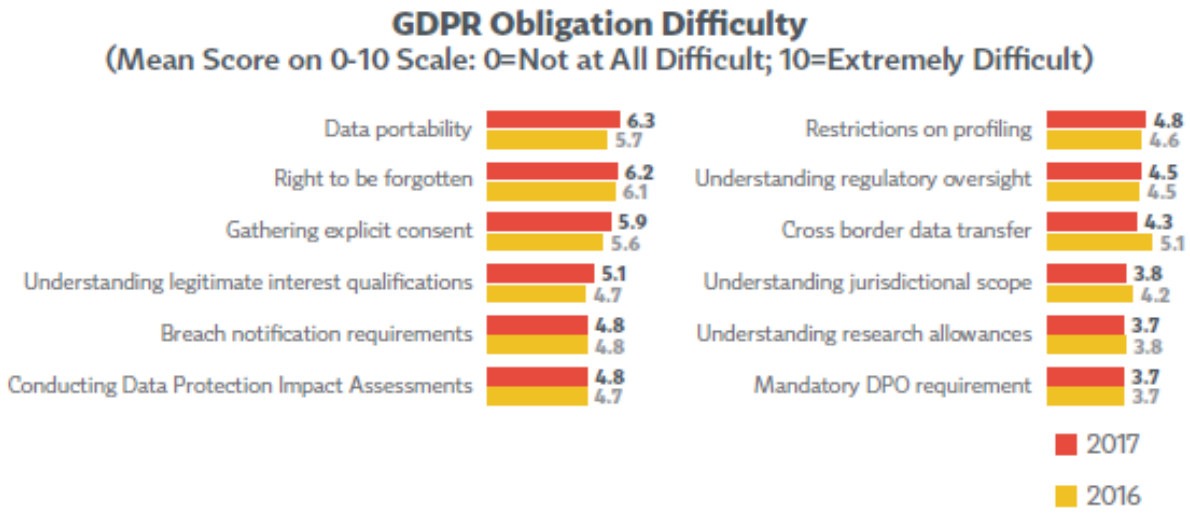
- Artikkel 36 nr. 5 gir medlemstatene adgang til å fastsette ytterligere plikt til forhåndsdrøftinger dersom opplysninger behandles til utførelse av en oppgave i allmennhetens interesse.
- "Etter departementets syn er det vanskelig i dag å overskue hvordan plikten til forhåndsdrøftelse vil utvikle seg og om det er nødvendig å utvide plikten til å gjelde andre områder. Det kan også være nødvendig eller hensiktsmessig å presisere nærmere hvilke type behandlinger som krever forhåndsdrøftinger. Departementet foreslår på denne bakgrunn en forskriftshjemmel som kan brukes til nærmere regulering av plikten til forhåndsdrøftinger, se lovutkastet § 11."

HØGSKOLEN I OSLO OG AKERSHUS

Sanksjoner

- Ved overtredelser av den behandlingsansvarliges og databehandlerens forpliktelser i henhold til bl.a. artikkel 35 og 36:
  - Administrative bøter på opptil € 10M eller på opptil 2% av den samlede globale årsomsetningen i forutgående regnskapsår, der det høyeste beløpet anvendes
- Ved manglende overholdelse av et pålegg fra DT som nevnt i artikkel 58 nr. 2 (art. 83 nr. 6) eller dersom det ikke gis tilgang i strid med artikkel 58 nr. 1 (art. 83 nr. 5 bokstav e):
  - Administrative bøter på opptil € 20M eller på opptil 4% av den samlede globale årsomsetningen i forutgående regnskapsår, der det høyeste beløpet anvendes

HØGSKOLEN I OSLO OG AKERSHUS



(Source: IAPP-EY Annual Privacy Governance Report 2017 p. xix)

HØGSKOLEN I OSLO
OG AKERSHUS

Takk for oppmerksomheten!