GDPR

Advokat Kari Gimmingsrud

Haavind

Velkommen!

Agenda

1. EUs nye forordning – sentrale endringer og hva betyr det for virksomhetene v/Haavind

2. Adeccos erfaringer fra arbeidet med implementeringen

3. Vesentlige endringer og tekniske utfordringer v/Pitney Bowes

Hvorfor endre reglene?

EU-kommisjonen:

It’s about trust…

and helping business boom

EUs personvernforordning

- Vil bli gjort gjeldende i Norge gjennom EØS-avtalen
- Trer i kraft i EU 25. mai 2018
- «One continent one law» - «One stop shop»
- Hvor stort spillerom får landene i EU (EØS)?
  - En del unntak og muligheter for nasjonal tilpasning, for eksempel forordningen art. 88 «*Processing in the context of employment*»
- En del vil være som i dag, men også mye nytt

Viktige endringer

- Utvidet anvendelsesområde
- Flere rettigheter for datasubjektene
- Strengere forpliktelser for virksomhetene, også databehandlere
- Klare og strenge informasjonsforpliktelser ved avvik
- Personvernombud vil bli pålagt for en del virksomheter
- Sanksjoner – i en helt annen skala

Hvem gjelder den for?

- Virksomheter som er etablert i EU (EØS)

- Virksomheter etablert utenfor EU (EØS) som
  - Tilbyr varer eller tjenester til individer i EU (EØS), eller
  - Overvåker atferden til individer som finner i sted innenfor EU (EØS)

Personopplysninger

- Navn
- Adresse
- Bilde
- Lokalisering
- IP-adresse
- Online identifier
- Helseinformasjon

mm.

Forordningen art. 4 (1):

'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an ***identifier*** *such as a name, an identification number,* ***location data****, an* ***online identifier*** *or to one or more factors specific to the physical, physiological,* ***genetic****, mental, economic, cultural or social identity of that natural person*

Sentrale begreper

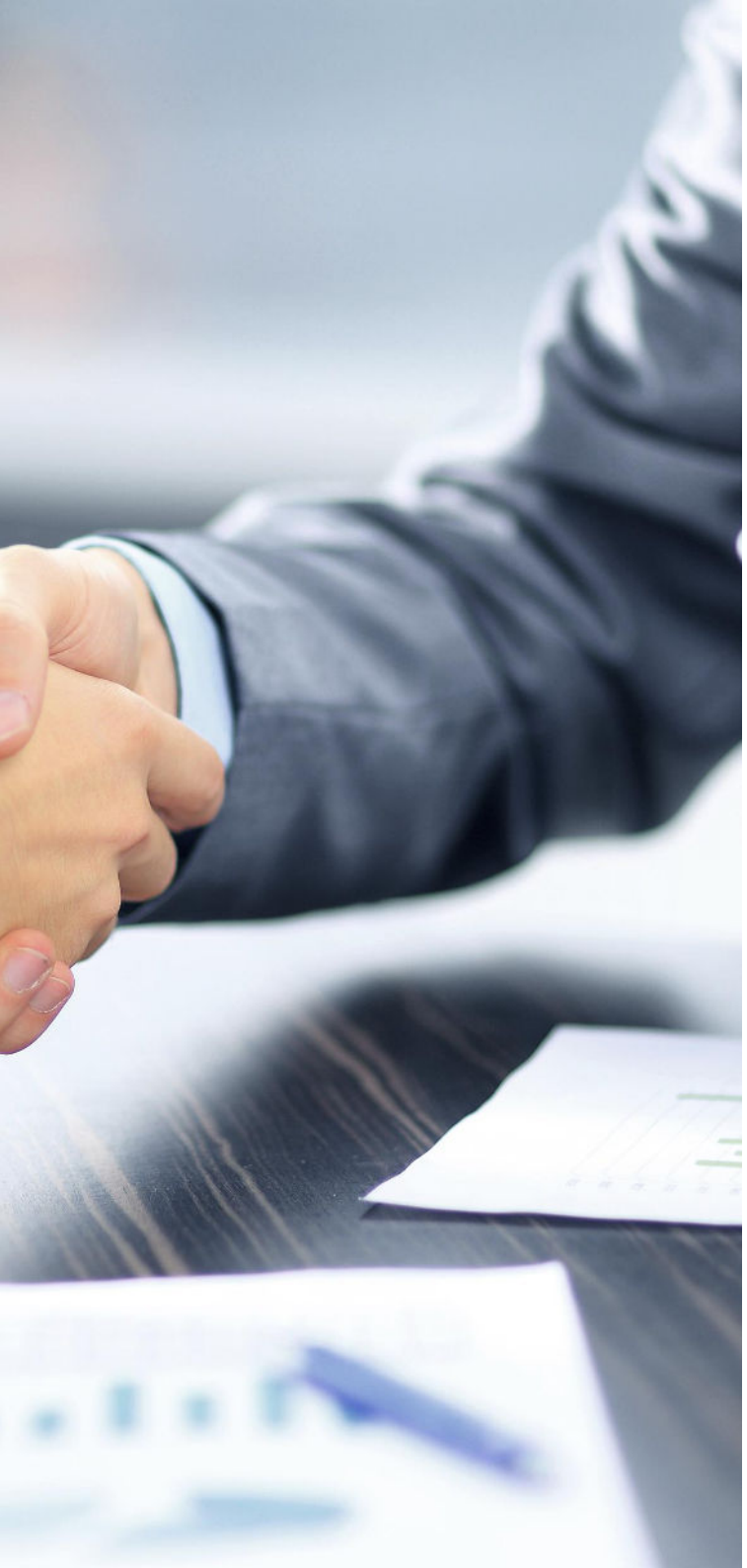
Personal data	any information relating to an identified or identifiable natural person (‘data subject’)
Special categories of personal data	processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
Controller	the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data
Processor	processes personal data on behalf of the controller
Processing	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means

Mindre byråkrati

- «One stop shop»
- Dagens melde- og konsesjonsplikt bortfaller
- I noen tilfeller en konsultasjonsplikt med Datatilsynet
- Noen forenklinger og færre «tyngende» forpliktelser for SME, men ikke ubetinget

Behandlingsgrunnlag

- Den som behandler personopplysninger er underlagt omfattende forpliktelser
- Må ha et lovlig behandlingsgrunnlag for all behandling av personopplysninger
- Strengere krav for «særlige kategorier» av personopplysninger
- Barns samtykke



Bruk av samtykke som behandlingsgrunnlag

«freely given, specific, informed and unambiguous»

- Datasubjektene må få informasjon før de samtykker
- Behandlingsansvarlig må kunne dokumentere at samtykke er gitt

Rettigheter for datasubjektene

- Klare rettigheter – og noen nye
  - Rett til informasjon
  - Rett til innsyn
  - Retting og sletting
  - Rett til å begrense behandling
  - Dataportabilitet
  - Motsette seg profilering
  - Begrense og motsette seg markedsføring
  - Få beskjed hvis noe går galt
  - Osv.

Internkontroll og informasjonssikkerhet

- Kartlegging og oversikt «records»
- Internkontroll og dokumentasjon
- Risikovurderinger
- Informasjonssikkerhet

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms… the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk

Konsekvensanalyse

«høy risiko»

Privacy by design and default

The controller shall implement appropriate technical and organisational measures in an effective way in order to meet the requirements of this Regulation and protect the rights of data subjects

Databehandlere

- Mer detaljerte krav til databehandleravtalen
- Samarbeid
- Datasubjektene kan henvende seg til databehandler
- Tilsynsmyndigheten

Strengere forpliktelser ved avvik

- Rapport til myndighetene innen 72 timer fra avviket ble oppdaget
- Informasjon til de registrerte «høy risiko»
- Databehandlers forpliktelser

Personvernombud

- Flere virksomheter må ha personvernombud, artikkel 37
  - «public authority or body»
  - Kjerneaktiviteten forutsetter «regular and systematic monitoring of data subjects on a large scale»
  - Kjerneaktivitet er behandling av «special categories of personal data» on a large scale

- Krav til organisering og «uavhengighet»

  DPOs cannot fulfil duties outside the scope of data protection which would "result in a conflict of interest". Senior management positions which involve decision-making around how and why personal data is used will conflict with the role of the DPO.

Konsekvensene av manglende overholdelse av regelverket

- Lokale tilsynsmyndigheter overvåker
- Arbeidet er koordinert på EU nivå
- Kostnadene ved å ikke overholde regelverket kan være betydelig

Bilde/oversikt fra EU-kommisjonen

Hva skjer videre og hvordan forberede seg?

Spørsmål?

Kari Gimmingsrud
Advokat
Mob: 922 91 006
E-post: k.gimmingsrud@haavind.no