

Informasjonsplikten – når, hva og hvordan?

Katrine Blixrud, Senior Privacy Officer,
Group Compliance, Group Privacy Office



Påstand

«Informasjonsplikten er oppfylt når man har publisert en personvernerklæring som er lett tilgjengelig på hjemmesiden til virksomheten»

Agenda



Relevante personvernprinsipper



Overordnede krav i GDPR artikkel 12



Når, hva og hvordan informere?

Personvernprinsippene: Åpenhet og rettferdighet



Forutsigbarhet



Tillit



Utgangspunktet for ivaretagelse av øvrige rettigheter

Overordnede krav – GDPR artikkel 12



Kort om noen aktuelle saker

Bot til Caixabank for vage og uklare formuleringer i personvernerklæringen

Varsel om overtredelsesgebyr til Disqus for manglende oppfyllelse av informasjonsplikten



Informasjonsplikten

Når?

Hva?

Hvordan?

Når skal informasjon gis?

- Samtidig med at opplysningene samles inn fra den registrerte selv
- Senest innen én måned etter at opplysningene er samlet inn fra andre enn den registrerte selv
- Ved endringer av en viss karakter



Hva skal det gis informasjon om?

Omfattende krav i GDPR artikkel 13 og 14

Lov om behandling av personopplysninger (personopplysningsloven)

Artikkel 13. Informasjon som skal gis ved innsamling av personopplysninger fra den registrerte

1. Når personopplysninger om en registrert samles inn fra den registrerte, skal den behandlingsansvarlige på tidspunktet for innsamlingen av personopplysningene gi den registrerte følgende informasjon:
 - a) identiteten og kontaktopplysningene til den behandlingsansvarlige og eventuelt den behandlingsansvarliges representant,
 - b) kontaktopplysningene til personvernombudet, dersom dette er relevant,
 - c) formålene med den tiltenkte behandlingen av personopplysningene samt det rettslige grunnlaget for behandlingen,
 - d) dersom behandlingen er basert på artikkel 6 nr. 1 bokstav f), de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart,
 - e) eventuelle mottakere eller kategorier av mottakere av personopplysningene,
 - f) dersom det er relevant, det faktum at den behandlingsansvarlige akter å overføre personopplysninger til en tredjestat eller en internasjonal organisasjon og om hvorvidt Kommisjonen har truffet en beslutning om tilstrekkelig beskyttelsesnivå eller ikke, eller når det gjelder overføringene nevnt i artikkel 46 eller 47 eller artikkel 49 nr. 1 annet ledd, en henvisning til nødvendige eller passende garantier, hvordan man får tak i et eksemplar av dem, eller hvor de er gjort tilgjengelig.
2. I tillegg til informasjonen nevnt i nr. 1 skal den behandlingsansvarlige på tidspunktet for innsamling av personopplysninger gi den registrerte følgende ytterligere informasjon som er nødvendig for å sikre en rettferdig og åpen behandling:
 - a) det tidsrom personopplysningene vil bli lagret, eller dersom dette ikke er mulig, kriteriene som brukes for å fastsette dette tidsrommet,
 - b) retten til å anmode den behandlingsansvarlige om innsyn i og retting eller sletting av personopplysninger eller begrensning av behandlingen som gjelder den registrerte, eller til å protestere mot behandlingen samt retten til dataportabilitet,
 - c) dersom behandlingen er basert på artikkel 6 nr. 1 bokstav a) eller artikkel 9 nr. 2 bokstav a), retten til når som helst å trekke tilbake et samtykke uten at det påvirker lovligheten av en behandling basert på et samtykke før samtykket trekkes tilbake,
 - d) retten til å klage til en tilsynsmyndighet,
 - e) om det foreligger et lovfestet eller avtalefestet krav om å gi personopplysninger eller et krav som er nødvendig for å inngå en avtale, samt om den registrerte har plikt til å gi personopplysningene og om mulige konsekvenser dersom vedkommende ikke gjør det,
 - f) forekomsten av automatiserte avgjørelser, herunder profilering, som nevnt i artikkel 22 nr. 1 og 4, og, i det minste i nevnte tilfeller, relevant informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte.
3. Dersom den behandlingsansvarlige har til hensikt å viderebehandle personopplysningene for et annet formål enn det opplysningene ble samlet inn for, skal den behandlingsansvarlige for nevnte viderebehandling gi den registrerte informasjon om nevnte andre formål og annen nødvendig informasjon som nevnt i nr. 2.
4. Nr. 1, 2 og 3 får ikke anvendelse dersom og i den grad den registrerte allerede har informasjonen.

WhatsApp-saken

- Det irske datatilsynet fant brudd på en rekke av informasjonspliktene i GDPR
- Flere tilsyn i Europa protesterte på utkastet til vedtak – ikke strengt nok
- Saken havnet hos Personvernrådet som fant flere brudd på informasjonspliktene

Hvordan

Virksomheten må selv finne
en passende form å gi informasjon på,
innenfor visse rammer

Virksomheten må aktivt "gi" den
enkelte informasjonen

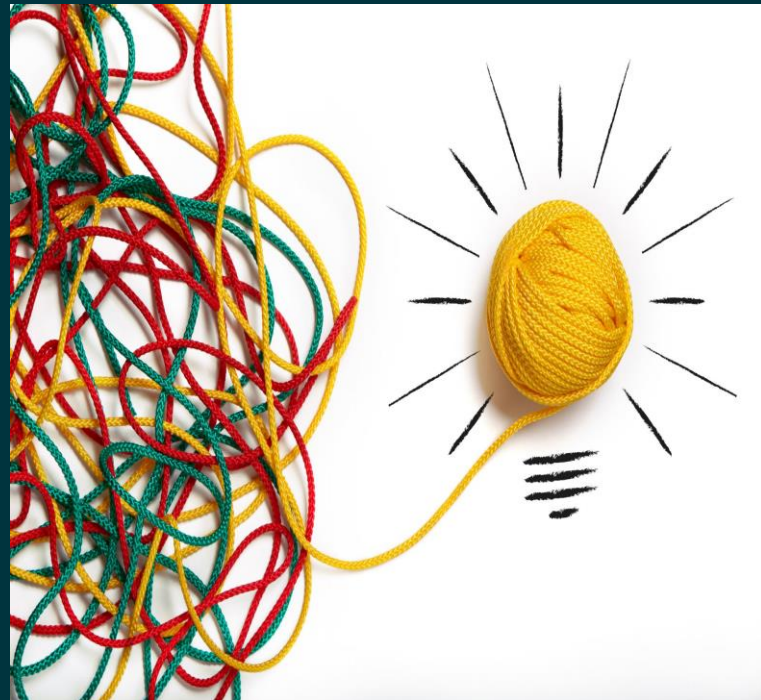
Krav til form?



Hvordan

Hvordan forene krav til å gi kortfattet og forståelig informasjon

- og samtidig få med alle krav til innhold i GDPR artikkel 13 og 14?



Lagvis informasjon

EDPB og Datatilsynet anbefaler at første lag gir informasjon om:

- formålet med behandlingen
- virksomhetens identitet
- den enkeltes rettigheter
- informasjon om behandling av personopplysninger som kan ha særskilt stor innvirkning på den enkelte eller fremstå som overraskende



Påstand

«Informasjonsplikten er oppfylt når man har publisert en personvernerklæring som er lett tilgjengelig på hjemmesiden til virksomheten»

Takk for meg!