Introduksjon til GDPR

Del 1

1

Introduksjon til GDPR

«Å lykkes med ideene bak GDPR er et av premissene for å lykkes med mennesker. Det viktigste er å fortjene og å oppnå tillit hos kunder og brukere.»

«Med fokus, bevissthet, rett kompetanse i alle ledd og ikke minst en forståelse for data, går ikke dette bare i orden, det har alle muligheter til å gå bra. Godt GDPR-arbeid!» (Jarbekk og Sommerfeldt, 2020)

2

GDPR introduksjon

- Art. 1-4 Alminnelige bestemmelser
- Art. 5-11 Prinsipper
- Art. 12-23 Den registrertes rettigheter
- Art. 24-43 Behandlingsansvarlig og databehandler

3

Bruk din vurderingsevne

«Bestemmelsene gir med andre ord få klare 'ja' eller 'nei', men er i utpreget grad **vurderingspregede** med rom for å kunne argumentere for ønskede løsninger.»
(Schartum, 2020)

4

Markedsføringsloven §15

§ 15. ***Begrensninger i bruk av visse kommunikasjonsmetoder***

I næringsvirksomhet er det forbudt, uten mottakerens forutgående samtykke, å rette markedsføringshenvendelser til fysiske personer ved elektroniske kommunikasjonsmetoder som tillater individuell kommunikasjon, som for eksempel elektronisk post, telefaks eller automatisert oppringningssystem (talemaskin).

Krav om forhåndssamtykke etter første … for markedsføring der den fysiske personen kontaktes muntlig ved telefon.

Krav om forh… der den næringsd… gjelde den næring… elektroniske adres… gis anledning til å …

Med elektron… elektronisk kommu… omfattes tekst- og multimediemeldinger til mobiltelefon.

Ehandelslovens bestemmelser, herunder § 9 om elektronisk markedsføring, gjelder i tillegg til bestemmelsen her.

… forbudt, uten mottakerens **forutgående samtykke**, å rette markedsføringshenvendelser til fysiske personer ved elektroniske kommunikasjonsmetoder …

5

InfoCuria
Case-law

English (en)

…ce Article 1 of the Privacy Shield Decision is inseparable from Articles 2 and 6 of, and the annexes to, that decision, its invalidity affects the validity of the decision in its entirety.

…he light of all of the foregoing considerations, it is to be concluded that the Privacy Shield Decision is invalid.

… to whether it is appropriate to maintain the effects of that decision for the purposes of avoiding the creation of a legal vacuum (see, to that effect, judgment of 28 April 2016, *Borealis Polyolefine and …thers*, C-191/14, C-192/14, C-295/14, C-389/14 and C-391/14 to C-393/14, EU:C:2016:311, paragraph 106), the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy …cision such as the Privacy Shield Decision is not liable to create such a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the …sence of an adequacy decision under Article 45(3) of the GDPR or appropriate safeguards under Article 46 of the GDPR.

…osts

…nce these proceedings are, for the parties to the main proceedings, a step in the action pending before … …servations to the Court, other than the costs of those parties, are not recoverable.

… must be interpreted as meaning …

…n those grounds, the Court (Grand Chamber) hereby rules:

Article 2(1) and (2) of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) must be interpreted as meaning that that regulation applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defence and State security.

Article 46(1) and Article 46(2)(c) of Regulation 2016/679 must be interpreted as meaning that the appropriate safeguards, enforceable rights and effective legal remedies required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded a level of protection essentially equivalent to that guaranteed within the European Union by that regulation, read in the light of the Charter of Fundamental Rights of the European Union. To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, take into consideration both the contractual clauses agreed between the controller or processor established in the European Union and the

6

Lov om behandling av personopplysninger (personopplysningsloven)

Dato	LOV-2018-06-15-38
Departement	Justis- og beredskapsdepartementet
Sist endret	LOV-2018-12-20-116
Ikrafttredelse	20.07.2018
Endrer	LOV-2000-04-14-31
Kunngjort	15.06.2018
Rettet	11.02.2019 (PVF art 40)
Korttittel	Personopplysningsloven

Jf. *tidligere* lov 14. april 2000 nr. 31. – Jf. EØS-avtalen vedlegg XI nr. 5e (forordning (EU) 2016/679 – personvernforordningen, også omtalt som GDPR og PVF).

Kapitteloversikt:

Kapittel 1. Personvernforordningen (§1)

Kapittel 2. Lovens saklige og geografiske virkeområde (§§ 2 - 4)

Kapittel 3. Utfyllende regler om behandling av personopplysninger (§§ 5 - 15)

Kapittel 4. Unntak fra den registrertes rettigheter (§§ 16 - 17)

Nasjonale lover
(i tillegg til GDPR)

7

Person-opplysnings-loven

«Fordi forordningen skal praktiseres likt i alle EØS-land, er det i utgangspunktet ikke tillatt å la bestemmelser i forordningen **«flyte ut»** i nasjonal lovgivning» (Schartum, 2020)

8

Personvernrådet

For å **påvise at** den behandlingsansvarlige **overholder denne forordning**, særlig med hensyn til kartlegging av risikoen, samt kartlegging av beste praksis for å redusere risikoen, kan særlig gis ved hjelp av **retningslinjer fra Personvernrådet** eller anvisninger fra et personvernombud.

9

edpb
European Data Protection Board

HOME ABOUT EDPB NEWS OUR WORK & TOOLS

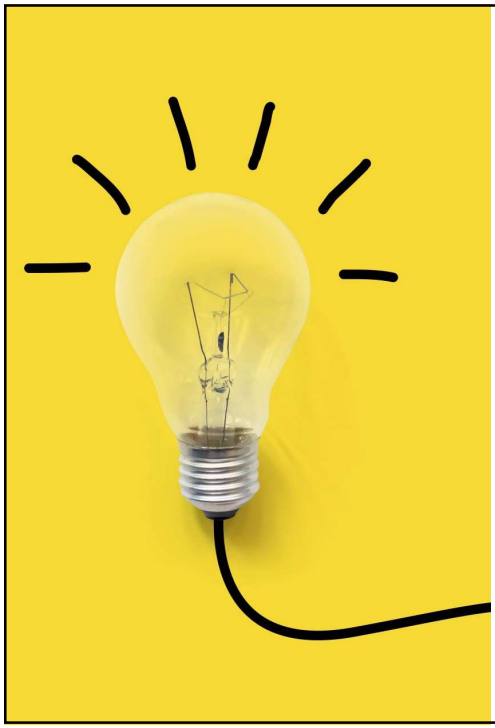
European Data Protection Board > Our Work & Tools > General Guidance > GDPR: Guidelines, Recommendations, Best Practices

GDPR: Guidelines, Recommendations, Best Practices

- Guidelines 08/2020 on the targeting of social media users - version for public consultation
- Guidelines 07/2020 on the concepts of controller and processor in the GDPR - version for public consultation
- Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR - version for public consultation
- Guidelines 05/2020 on consent under Regulation 2016/679
- Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak

10

11

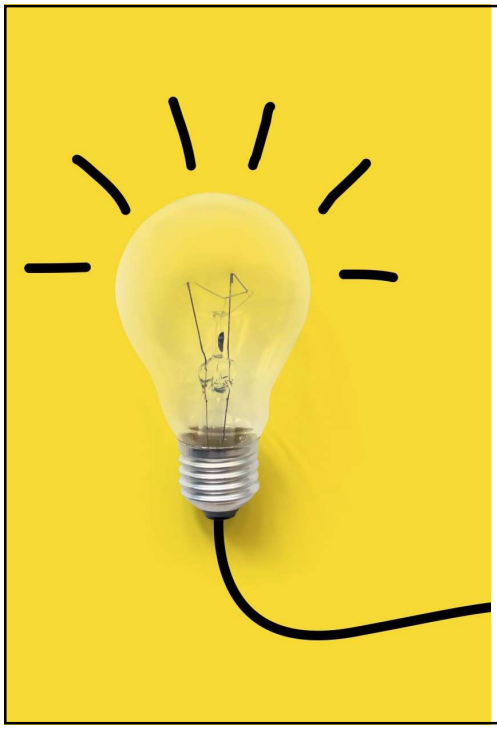


Til hvem skal personvernreglene kommuniseres?

A. Til ansatte som er direkte involvert i personvern
B. Bare til toppledelsen
C. Til alle ansatte i virksomheten
D. Til personvernombudet

- C. Til alle ansatte i virksomheten

12

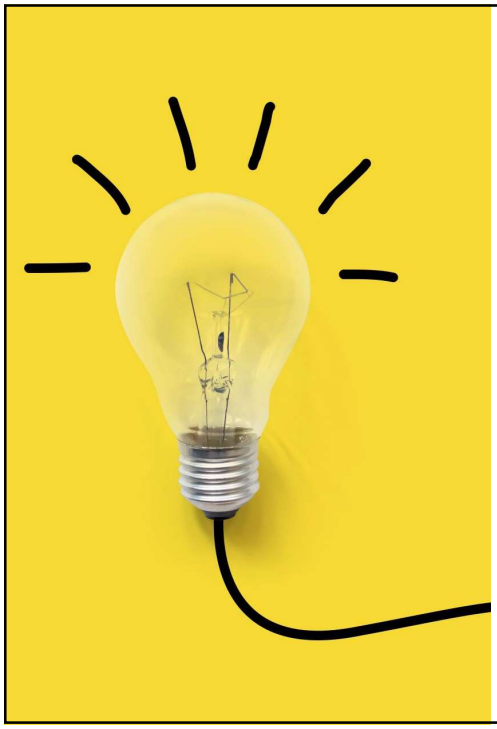


Hva er Datatilsynets rolle?

A. Sikre at GDPR blir anvendt på en konsekvent måte
B. Sikre at virksomheter overholder enkeltpersoners rettigheter
C. Å ta bindende avgjørelser i samarbeid med Personvernrådet
D. Å gi retningslinjer for hvordan man tolker prinsippene i GDPR

- B. Sikre at virksomheter overholder enkeltpersoners rettigheter

13

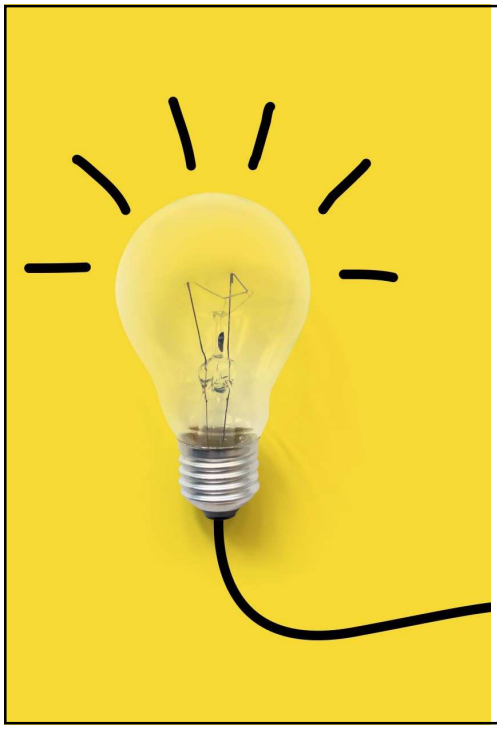


Hvorfor bestemte EU seg for å vedta GDPR?

A. For å lovbestemme ansvaret til behandlingsansvarlig
B. Å forenkle fri flyt av data mellom EU land
C. Å forenkle fri flyt av data utenfor EU
D. Å fremme samarbeidet med andre land utenfor EU

- B. Å forenkle fri flyt av data utenfor EU

14

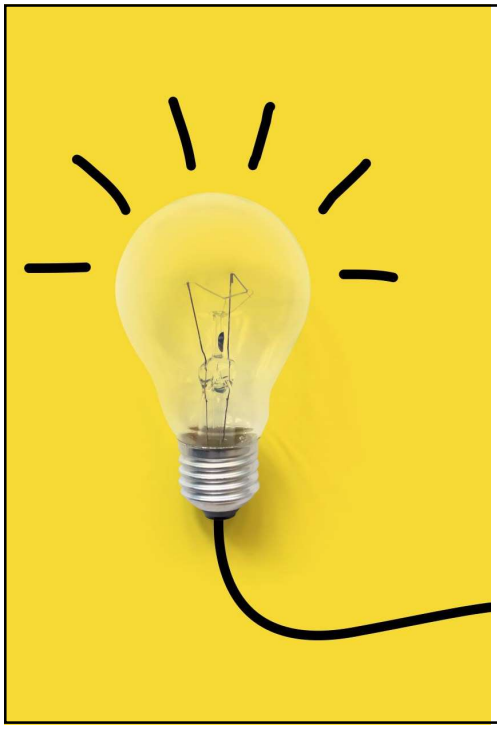


Virksomheter kan bli bøtelagt med opptil EUR 20 millioner eller 4% global omsetning hvis de ikke overholder GDPR.

- Rett
- Galt

- Rett

15

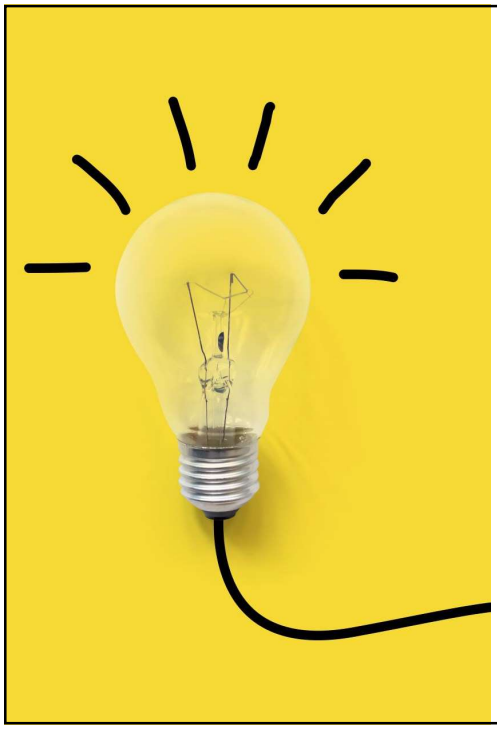


4% bot av global omsetning; omfatter det alle enhetene i en multinasjonal organisasjon?

- Rett
- Galt

- Rett

16



Hvilken del av GDPR kommer med betraktninger og veiledning slik at den blir bedre forstått?

A. Fortale 1 – 173
B. Artikler 1 – 99
C. Sentrale forskrifter
D. EØS-avtalen

- A. Fortale 1 – 173

17

Saklig og geografisk virkeområde

Del 2

18

Grunnleggende, generelle krav til behandlingsopplegget

- Hvilke **personopplysninger** ønsker jeg å behandle?
- Til hvilket **formål** ønsker jeg å bruke personopplysningene?
- Hvilket **rettslig grunnlag** kan jeg påberope meg?
- Hvordan må/kan jeg **organisere** behandlingen av personopplysninger?
- Hvordan må/kan jeg **sikre** behandlingen av personopplysninger?
- Gir den planlagte behandlingen **akseptabel risiko** for registrerte personers rettigheter og friheter?
- Hvordan kan jeg **påvise/dokumentere** at jeg har forsøkt å etterleve GDPR?

19

Art. 3(1) Geografisk virkeområde

Denne forordning får anvendelse på behandling av personopplysninger som utføres i forbindelse med aktivitetene ved virksomheten **til en behandlingsansvarlig** eller en databehandler **i Unionen**, *uavhengig av om behandlingen finner sted i Unionen eller ikke*.

20

Art. 3(2) Geografisk virkeområde

Denne forordning får anvendelse på behandling av personopplysninger om registrerte **som befinner seg i** Unionen, og som utføres av en behandlingsansvarlig eller databehandler som **ikke er etablert** i Unionen, dersom behandlingen er knyttet til:

a) tilbud av **varer eller tjenester** til slike registrerte i Unionen, *uavhengig av om det kreves betaling* fra den registrerte eller ikke, eller

b) monitorering av deres atferd, i den grad deres atferd finner sted i Unionen.»

21

Tilbud av varer eller tjenester

For å avgjøre om det tilbys varer eller tjenester til registrerte som befinner seg i Unionen, bør det bringes på det rene om det er **åpenbart** at den behandlingsansvarlige **har til hensikt…**

22

Monitering av atferd

For å fastslå om en behandlingsaktivitet kan anses som monitorering av de registrertes atferd bør det bringes på det rene om det skjer **sporing av fysiske personer på internett**, herunder en mulig påfølgende bruk av teknikker for behandling av personopplysninger som innebærer **profilering** av en fysisk person, særlig **med det formål å treffe avgjørelser** om vedkommende eller analysere eller forutsi vedkommendes personlige preferanser, atferd eller holdninger.

23

Oppgaver: Gjelder GDPR?

24

Et programvareselskap i India, med kunder over hele verden, tjener penger på sin søkemotor ved å tilby tilpassede annonser. Programmet som benyttes kombinerer nøkkelord som det søkes på og IP-adresse.

- Ja, de behandler personopplysninger om registrerte som befinner seg i Unionen, selv om de ikke er etablert i Unionen. Behandlingen er knyttet til tilbud av tjenester til slike registrerte, selv om det ikke kreves betaling. Det er dessuten monitorering av atferd med sporing og profilering av de registrerte.

25

TwoDrive tilbyr lagring i skyen til bedriftskunder. En kursleverandør har behov for 325 terabyte med lagring av personopplysninger på alle deltakere fra tidenes morgen. TwoDrive er registrert i USA, og kursleverandøren har hovedkontor i Oslo.

Ja. Kundens sin behandling av personopplysninger utføres i forbindelse med aktivitetene i EU/EØS.

Det kan på den annen side argumenteres for kanskje ikke. De tilbyr ikke tjenester til registrerte personer i EU/EØS, men at tjenesten er et tilbud kun til kunden, altså selve virksomheten.

26

Behandling av personopplysninger

Del 3

27

Personopplysning

Enhver opplysning om en **identifisert** eller **identifiserbar** fysisk person («den registrerte»); en identifiserbar fysisk person er en person som **direkte** eller **indirekte** kan identifiseres, særlig ved hjelp av en identifikator.

28

Personopplysning

- Om et menneske som kan pekes ut
  - **Identifisert**
    - «David Jacobsen liker Tromsø. Han bodde i Gausdalsvegen 17 i perioden 1987 til 1989»
  - **Identifiserbar**
    - «En mann som ble født 220968 i Bergen, flyttet til Arendal 2 måneder gammel, og bor nå på postnummer 4083»

29

Personopplysning

- **Om et menneske som kan pekes ut**
  - Direkte eller indirekte
  - Navn, id-nummer, lokasjon, ip-adresse
  - Identifisere en person ved samkjøring av to eller flere registre

30

Identifiserbar

«Jo flere slike identifiserende elementer vi kan spesifisere og kombinere, jo færre personer passer til beskrivelsen, og til slutt er identifiseringen entydig»

31

Fortale 26

- Personopplysninger som er blitt **pseudonymisert**, og som kan knyttes til en fysisk person ved hjelp av tilleggsopplysninger, bør anses som opplysninger om en identifiserbar fysisk person.
- Det bør tas hensyn til alle midler som det med rimelighet kan tenkes at den behandlingsansvarlige kan ta i bruk for å identifisere vedkommende **direkte eller indirekte.**
- Det bør tas hensyn til alle objektive faktorer, f.eks. teknologien.

32

Pseudonymisering

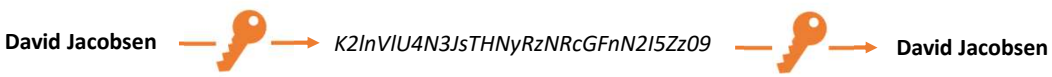
- **Tokenization**
  - Bytter ut et personnummer med en tilfeldig valgt identifikator
    - *01010149939 = 4545435*
  - Kundeopplysninger lagres forskjellig avhengig av tilgang

Adgangsområde 1	Adgangsområde 2
Personnummer	Token
Navn	Opprettet dato
Fødselsdato	
Token	

33

Pseudonymisering

- **Kryptering**
  - Navn gjøres ugjenkjennelig
  - Noen kjenner nøkkelen og kan dermed gjenskape verdien



34

Anonymisering

Anonymiserte opplysninger = personopplysninger som er blitt behandlet på en slik måte at personen **ikke lenger kan identifiseres.**

35

Anonymisert?

Navn	Fødselsdato	Adresse	Besøksdato	Nøkkelkort aktivitet
~~John Doe~~	~~10.12.~~1982	~~Jane Lane 2~~, 0277 Bergen	23.04.2018	06:21 23:33
~~Jane Doe~~	~~11.02.~~1976	~~Veien gate~~, 0001 Oslo	22.04.2018	11:15 15:41 21:02 22:45
~~Jack Smith~~	~~01.03.~~2001	~~Olavs plass 19~~, Bodø	21.04.2018	11:15 19:45

36

Behandling

Enhver operasjon eller rekke av operasjoner **som gjøres med personopplysninger**, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring.

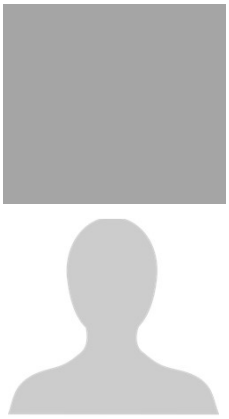
37

Unntak

Denne forordning **får ikke anvendelse** på behandling av personopplysninger som utføres av en fysisk person som ledd **i rent personlige eller familiemessige aktiviteter**.

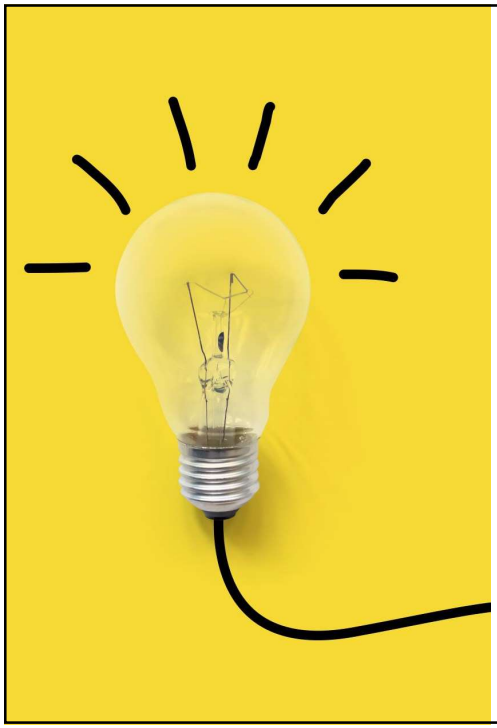
38

”Når vi bare har erstattet personopplysninger med en kode, så er det snakk om anonyme opplysninger, og derfor skal vi ikke lengre bekymre oss for GDPR”



- Jo, du må fortsatt være oppmerksom på GDPR.
- Selv om opplysninger som et navn eller en adresse er erstattet av en kode, f.eks.AB123, så er det fremdeles en personopplysning, hvis koden kan føres tilbake til den opprinnelige personopplysningen. Dette er situasjonen, så lenge det er noen som kan gjøre opplysningene lesbare og identifisere de personene det dreier seg om. Dette kalles ofte pseudonymiserte opplysninger, og slike opplysninger er omfattet av personvernreglene.
- Opplysninger er kun anonyme, og dermed ikke omfattet av personvernreglene, hvis ingen fysiske personer kan identifiseres ut fra opplysningerne eller i kombinasjon med andre opplysninger – og hvis anonymiseringen er ugjenkallelig.

39

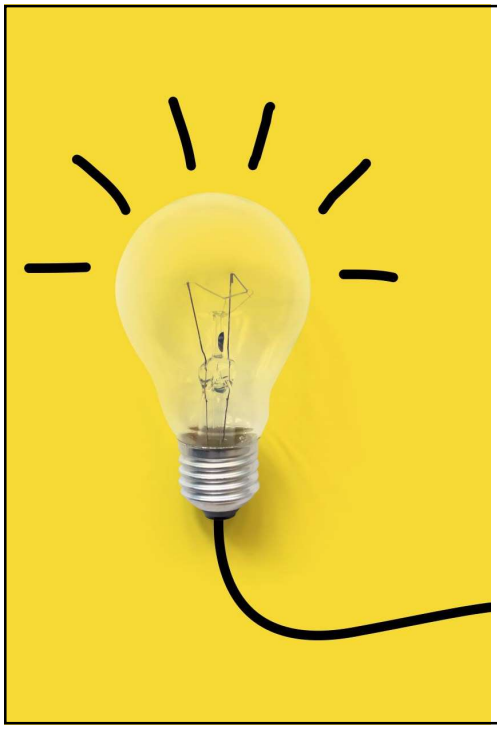


Hva identifiserer behandlingsaktiviteter?

A. Prosessen med å definere personene som skal behandle dataene.
B. Prosessen med å bestemme metodene for databehandling.
C. Prosessen med å etablere hvor dataene kommer fra, hvordan dataene blir behandlet og hvor dataene blir overført til.
D. Prosessen med å identifisere metodene for registrering av organisasjonens data.

- C. Prosessen med å etablere hvor dataene kommer fra, hvordan dataene blir behandlet og hvor dataene blir overført til.

40



Behandling av personopplysninger om straffedommer og lovovertredelser; under hvilke omstendigheter skal den utføres?

A. Ved utførelse av en oppgave som er av offentlig interesse
B. Hvis tillatt i henhold til nasjonal rett som sikrer rettigheter og friheter
C. Når den registrerte har gitt eksplisitt samtykke
D. Hvis nødvendig for å beskytte de berettigede interesser

- B. Hvis tillatt i henhold til nasjonal rett som sikrer rettigheter og friheter

41

Behandlingsansvarlig og databehandler

Del 4

42

Behandleransvarlig

Bestemmer formålet med behandlingen av personopplysninger og **hvilke midler** som skal benyttes.

43

Databehandler

Behandler personopplysninger **på vegne av** den behandlingsansvarlige.

44

Artikkel 26. Felles behandlingsansvarlige

Dersom to eller flere behandlingsansvarlige **i fellesskap fastsetter formålene med og midlene** for behandlingen, skal de være felles behandlingsansvarlige

45

Spør deg selv

1. Har din virksomhet kjennskap til de nye GDPR reglene?
2. Hvilke personopplysninger behandler dere?
3. Hvilken informasjon gir dere de registrerte?
4. Hvordan oppfyller dere de registrertes rettigheter?
5. På hvilket rettslig grunnlag behandler dere personopplysninger?
6. Hvordan innhenter dere samtykke?
7. Behandler dere personopplysninger om barn?
8. Hva skal dere gjøre ved brudd på personvernet?
9. Er deres behandlinger forbundet med særlige risiko?
10. Har dere tiltenkt personvern i deres it-systemer?
11. Hvem er ansvarlig for personvernspørsmål i deres virksomhet?
12. Driver dere virksomhet i flere land?

46

Oppgaver: Hvem er behandlingsansvarlig?

47

Du ser et behov for å markedsføre virksomhetens tjenester. Du kontakter et markedsføringsselskap og avtaler at selskapet skal sende ut markedsføring til kundene dine.

Det er du som har bestemt å behandle personopplysninger for markedsføring. De konkrete personopplysninger ville ikke blitt behandlet for markedsføring med mindre du ba markedsføringsselskapet dette. Du er derfor behandlingsansvarlig.

Markedsføringsselskapet har sine egne metoder, og du kan derfor ikke instruere dem. Markedsføringsselskapet er derfor behandlingsansvarlig.

48

Et rekrutteringsselskap mottar jobbsøknadene fra kunden. Deretter vurderer rekrutteringsselskapet søknadene på vegne av kunden (for eksempel bakgrunnssjekk), men får ikke bruke informasjonen om kandidatene til egne formål (for eksempel lagre informasjonen i egen database).

I så fall er rekrutteringsselskapet databehandler, og kunden behandlingsansvarlig.

49

Et rekrutteringsselskap har en egen database. I databasen plukker selskapet ut egnede kandidater for en stilling som kunden ønsker besatt. Rekrutteringsselskapet står for søk, kartlegging og innhenter CV og referanser. Kunden bestemmer tilslutt hvem som skal ansettes.

- Her har rekrutteringsselskapet og kunden i felleskap bestemt formål (ansettelse hos kunden) noe som taler for at de er felles behandlingsansvarlige.

50

Du er plaget med innbrudd i butikken din og setter derfor opp et overvåkingskamera. Du ber et vaktselskap om å lagre opptak, og undersøke opptakene om det skjer noe mistenkelig.

- Vaktselskapet behandler opptakene på vegne av deg, og er derfor databehandler. Du er på din side behandlingsansvarlig.

51

To butikker holder til i samme bygg og har felles inngang. Ved gjentatte tilfeller er butikkene blitt plaget med innbrudd og har tapt store verdier. Butikkene bestemmer i felleskap å installere kameraovervåking ved fellesinngangen i en periode, og at opptak skal gjennomgås ved mistenkelige hendelser.

- Her har butikkene i felleskap bestemt formålet med kameraovervåkingen og hvordan overvåkingen skal gjennomføres. Dette tyder på at det foreligger et felles behandlingsansvar for kameraovervåkingen.

52

Som arbeidsgiver ber du en annen virksomhet sende ut lønnslipper på vegne av deg til dine ansatte.

- Du instruerer den andre virksomheten dette og hvordan utsendelsen skal skje. Den andre virksomheten kan ikke bruke opplysningene til egne formål. Du er derfor behandlingsansvarlig og virksomheten som sender ut lønnslipper er databehandler.

53

Reisebyrået «NiceTravel» tilbyr pakkereiser (fly og hotell) til sine kunder. For å kunne booke reisen og innkreve betaling, innhenter «NiceTravel» personopplysninger (navn, adresse, personnummer og kontoopplysninger) om kundene.

«NiceTravel» ber hotellet «GreatStay» om å booke hotellrom til kundene på de bestemte datoene. For at «GreatStay» skal kunne foreta sin behandling (reservere hotellrom) har hotellet bruk for noen av de samme personopplysningene om kundene. «NiceTravel» gir derfor videre disse opplysningene til «GreatStay».

«NiceTravel» ber dessuten flyselskapet «FlyNordic» om å reservere flyseter til kundene på de bestemte datoene. For at «FlyNordic» skal kunne foreta sin behandling (reservere flyseter) har «FlyNordic» også bruk for noen personopplysninger om kundenes navn og personnummer. «NiceTravel» gir derfor videre disse opplysningene til «FlyNordic».

- Reiseselskapet, hotellet og flyselskapet er hver især behandlingsansvarlig for den behandlingen de foretar.
- De behandler opplysningene til hver sine egne (nye) formål, og har selv vurdert hvilke opplysninger som er nødvendige for å foreta behandlingen.

54

En forelder laster opp et bilde på sin egen profil på et sosialt media, av en situasjon i barnehagen, så er det institusjonen og derfor kommunen, som er behandlingsansvarlig.

- Nei, selv om bildet er tatt i barnehagen, så er det forelderen, som har lastet opp bildet på sin egen profil, og derfor er det forelderen, som er ansvarlig for behandlingen for personopplysningen.

55

Virksomheten ønsker å utføre en statistikkundersøkelse der det blir behandlet personopplysninger, og vil benytte en elektronisk løsning. Virksomhetens ledelse ber en ansatt i virksomheten vurdere sikkerhetsmessige aspekter ved løsningen.

- Selv om virksomheten delegerer arbeidet til en ansatt er det virksomheten som er den behandlingsansvarlige, ikke den ansatte.

56

Prinsippene

Del 5

57

Formålsbegrensning

«Personopplysninger skal samles inn for **spesifikke, uttrykkelig angitte** og **berettigede formål** og ikke *viderebehandles på en måte som er uforenlig* med disse formålene»

58

Dataminimering

«Personopplysninger skal være **adekvate, relevante** og **begrenset** til det som er nødvendig for formålene de behandles for»

59

Riktighet

«Personopplysninger skal være **korrekte** og om nødvendig oppdaterte; det må treffes ethvert **rimelig tiltak** for å sikre at personopplysninger som er uriktige med hensyn til formålene de behandles for, uten opphold **slettes eller korrigeres**»

60

Korrigere hvis rimelig

Adresse: Sørskogen 3

- Sørskpgen 3
- Sørskogen 33

61

Lagringsbegrensning

«Personopplysninger skal lagres slik at det **ikke er mulig å identifisere** de registrerte **i lengre perioder** enn det som er **nødvendig for formålene** som personopplysningene behandles for»

62

Integritet og fortrolighet

«Personopplysninger skal behandles på en måte som **sikrer tilstrekkelig sikkerhet** for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av **egnede** tekniske eller organisatoriske **tiltak**.»

63

Lovlighet, rettferdighet og gjennomsiktighet

«Personopplysninger skal behandles på en **lovlig, rettferdig og gjennomsiktig** måte med hensyn til den registrerte»

64

Hvilket av alternativene nedenfor er i følge GDPR, ellers kjent som "dataminimering" - prinsippet?

A. Personopplysninger må være tilstrekkelige, relevante og begrenset til det som er nødvendig i forhold til formålene de blir behandlet for.
B. Personopplysninger må være nøyaktige og om nødvendig holdes oppdaterte.
C. Personopplysninger må kun skaffes til spesifiserte og lovlige formål.
D. Personopplysninger må håndteres på en sikker måte, inkludert vern mot ulovlig behandling eller utilsiktet tap, ødeleggelse eller skade.

A. Personopplysninger må være tilstrekkelige, relevante og begrenset til det som er nødvendig i forhold til formålene de blir behandlet for.

65

Hva sikrer prinsippet om ansvarlighet?

A. At behandlingsansvarlige overholder alle prinsippene i GDPR
B. At databehandlingen er basert på samtykke
C. At personopplysninger er beskyttet
D. At behandlingsansvarlige svarer på forespørsler fra en til tre måneder

A. At behandlingsansvarlige overholder alle prinsippene i GDPR

66

Formål uttrykkelig?

- En forening skriver at de bruker personopplysningene til medlemmene for administrasjon.
- Dette er for vagt.
- Foreningen kan f.eks. i stedet si at formålet med personopplysningene er å fakturere medlemsavgift, invitere medlemmene til foreningsmøte og dokumentere at virksomheten ikke jukser med medlemstall.

67

Formål uttrykkelig?

- Et nettsted oppgir at personopplysningene til brukerne kan anvendes for å tilby relevant kommunikasjon og en god brukeropplevelse.
- Dette er ikke i tråd med loven fordi det ikke er klart nok hva nettstedet vil anvende personopplysningene til.
- I stedet kan man heller si at nettstedet analyserer hva brukeren klikker på for å gi tilpasset markedsføring og avdekke hva slags funksjoner som er mest brukt, dersom det er tilfellet.

68

Behandlingsgrunnlag

Del 6

69

Artikkel 6. Behandlingens lovlighet

«Behandlingen er bare lovlig dersom og i den grad minst ett av følgende vilkår er oppfylt:

a) den registrerte har gitt **samtykke** til behandling av sine personopplysninger for ett eller flere spesifikke formål,

b) behandlingen er nødvendig for å **oppfylle en avtale** som den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse,

c) behandlingen er nødvendig for å oppfylle **en rettslig forpliktelse** som påhviler den behandlingsansvarlige,

d) behandlingen er nødvendig for å verne den registrertes eller en annen fysisk persons **vitale interesser**,

e) behandlingen er nødvendig for å utføre en oppgave **i allmennhetens interesse** eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt,

f) behandlingen er nødvendig for formål knyttet til de **berettigede interessene** som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn.»

70

Sensitive personopplysninger

- Gitt uttrykkelig samtykke
- Nødvendig av hensyn til viktige allmenne interesser
- Nødvendig i forbindelse med forebyggende medisin eller arbeidsmedisin
- Nødvendig av allmenne folkehelsehensyn
- Nødvendig for arkivformål i allmennhetens interesse

71

Samtykke

Enhver **frivillig**, **spesifikk**, **informert** og **utvetydig viljesytring** fra den registrerte der vedkommende ved en erklæring eller en tydelig bekreftelse gir sitt samtykke til behandling av personopplysninger som gjelder vedkommende.

72

Samtykke – artikkel 7

- Dersom behandlingen bygger på samtykke, skal den behandlingsansvarlige **kunne påvise** at den registrerte har gitt samtykke til behandling av personopplysninger om vedkommende.
- Dersom den registrertes samtykke gis i forbindelse med en skriftlig erklæring **som også gjelder andre forhold**, skal anmodningen om samtykke framlegges på en måte som gjør at **den tydelig kan skilles fra nevnte andre forhold**, i en forståelig og lett tilgjengelig form og på et klart og enkelt språk. Deler av en slik erklæring som er i strid med denne forordning, skal ikke være bindende.
- Den registrerte skal **ha rett til å trekke tilbake sitt samtykke** til enhver tid. Dersom samtykket trekkes tilbake, skal det ikke påvirke lovligheten av behandlingen som bygger på samtykket før det trekkes tilbake. Før det gis samtykke, skal den registrerte opplyses om dette. Det skal **være like enkelt å trekke tilbake** som å gi samtykke.
- Ved vurdering av om et samtykke er gitt frivillig skal det tas størst mulig hensyn til blant annet om oppfyllelse av en avtale, herunder om yting av en tjeneste, **er gjort betinget** av samtykke til behandling av personopplysninger som **ikke er nødvendig** for å oppfylle nevnte avtale.

73

Samtykke – fortale 32

Samtykke bør gis i form av **en tydelig bekreftelse der den registrerte på en frivillig, spesifikk, informert og utvetydig måte** gir sitt samtykke til behandling av vedkommendes personopplysninger, f.eks. i form av en skriftlig, herunder elektronisk, eller en muntlig erklæring. Dette kan innebære å krysse av i en boks under et besøk på et nettsted, velge tekniske innstillinger for informasjonssamfunnstjenester eller en annen erklæring eller handling som i denne forbindelse tydelig viser at den registrerte godtar den foreslåtte behandlingen av vedkommendes personopplysninger. **Taushet, forhåndsavkryssede bokser eller inaktivitet bør derfor ikke utgjøre et samtykke. Et samtykke bør omfatte alle behandlingsaktiviteter som utføres med henblikk på samme formål.** Dersom det er flere formål med behandlingen, bør det gis samtykke til alle. Dersom den registrertes samtykke skal gis etter en elektronisk anmodning, må anmodningen være tydelig, kortfattet og ikke unødig forstyrre bruken av den tjenesten samtykket gjelder.

74

Samtykke – fortale 43

For å sikre at et samtykke gis frivillig bør det ikke utgjøre et gyldig rettslig grunnlag for behandling av personopplysninger i et bestemt tilfelle **dersom det er en klar skjevhet mellom den registrerte og den behandlingsansvarlige**, særlig dersom den behandlingsansvarlige er en offentlig myndighet og det derfor er usannsynlig at samtykket er gitt frivillig med hensyn til alle omstendigheter som kjennetegner den bestemte situasjonen. Samtykket antas å ikke være gitt frivillig dersom det ikke er mulig å gi separat samtykke for forskjellige behandlingsaktiviteter, selv om det er hensiktsmessig i det enkelte tilfellet, eller dersom oppfyllelsen av en avtale, herunder yting av en tjeneste, avhenger av samtykket, til tross for at et slikt samtykke ikke er nødvendig for å oppfylle avtalen.

75

Nødvendig å oppfylle en avtale – artikkel 6.1.b.

Behandlingen er **nødvendig** for å oppfylle en avtale som den registrerte er **part i**, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse.

76

Rettslig forpliktelse – fortale 45

Dersom behandlingen utføres i samsvar med en **rettslig forpliktelse** som påhviler den behandlingsansvarlige, eller dersom behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet, bør behandlingen ha rettslig grunnlag i unionsretten eller medlemsstatenes nasjonale rett. Ved denne forordning kreves det ikke en særlig lovbestemmelse for hver enkelt behandling. **En lov kan være tilstrekkelig som grunnlag** for flere behandlingsaktiviteter som bygger på en rettslig forpliktelse som påhviler den behandlingsansvarlige, eller dersom behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet. Formålet med behandlingen bør også fastsettes i unionsretten eller i medlemsstatenes nasjonale rett.

77

Berettiget interesse

- Behandlingen er **nødvendig for formål** knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, **med mindre den registrertes interesser** eller grunnleggende rettigheter og friheter **går foran** og krever vern av personopplysninger, særlig dersom den registrerte er et barn.
- En berettiget interesse krever i alle tilfeller en nøye **vurdering**.

78

Offentlig interesse

Behandlingen er nødvendig for å **utføre en oppgave** i allmennhetens interesse eller **utøve offentlig myndighet** som den behandlingsansvarlige er pålagt.

79

Vitale interesser

Behandlingen av personopplysninger bør også anses som lovlig dersom den er nødvendig for å verne en interesse som er av avgjørende betydning for den registrertes eller en annen **fysisk persons liv**. Behandling av personopplysninger som er basert på en annen fysisk persons vitale interesser, bør i prinsippet bare finne sted dersom det er åpenbart at behandlingen ikke kan baseres på et annet rettslig grunnlag. Noen typer behandling kan tjene både viktige allmenne interesser og den registrertes vitale interesser, f.eks. når behandlingen er nødvendig av humanitære årsaker, herunder for å **overvåke epidemier og spredning av dem**, eller i humanitære nødssituasjoner, særlig i forbindelse med **naturkatastrofer** og menneskeskapte katastrofer.

80

Hovedpunkter

Samtykke
- Frivillig, spesifikk, informert og utvetydig viljesytring
- Må kunne trekkes tilbake
- Må ikke være en forutsetning for en urelatert tjeneste
- Kan ikke brukes når det er stor ubalanse av makt eller myndighet
- Må kunne dokumenteres
- Best å bruke når man gir «ekte valg» til de registrerte

Oppfylle en avtale
- Tolkes restriktivt (må «virkelig» være nødvendig)
- Du må påvise at det finnes en avtale, og etablere nødvendigheten

Berettiget interesse
- Ganske fleksibelt grunnlag
- GDPR definerer ikke hva slags interesser
- Gjennomføre en balansetest for å vise at den berettigede interessen ikke gjør inngrep i den registrertes interesser

81

Oppgaver: Gyldig samtykke?

82

Et selskap har en telefonkatalog over de ansatte, som er tilgjengelig for de ansatte via selskapets intranett. Selskapet vokser raskt og har nå rundt 700 ansatte. For å forbedre kommunikasjonen mellom ansatte ønsker bedriftens ledelse å gi den ansattes profil i telefonkatalogen et bilde av den ansatte. Ledelsen ber derfor hver ansatt om samtykke til å legge til et bilde i selskapets telefonkatalog.

- Hvis ledelsen understreker at det er helt frivillig og hvis den ansatte ikke ønsker å gi sitt samtykke, vil det ikke få negative konsekvenser for den ansatte. Ansattes samtykke vil bli ansett som frivillig.
- Hvis ledelsen i selskapet har informert de ansatte om at det vil få negative konsekvenser hvis de ikke gir samtykke, vil ikke samtykket være frivillig.

83

En elektronikkforhandler på nett gjør det til et vilkår for kjøp av mobiltelefoner at kunden må gi samtykke til at elektronikkforhandleren deler kundens informasjon med ulike teleselskaper. Kundens informasjon deles med teleselskapene med tanke på at selskapene kan sende kundene materiale om gunstige telefonabonnement. Deling av kundens informasjon er ikke nødvendig for kundens kjøp av mobiltelefonen.

- Kundens samtykke vil ikke bli ansett som frivillig hvis det er et vilkår for kjøp av telefonen.
- Elektronikkforhandleren kan be om samtykke til slik deling, men kunden må kunne nekte samtykke og samtidig beholde muligheten til å kjøpe varen.

84

En kunde abonnerer på nyhetsbrevet til en skobutikk med generelle rabatter. Skobutikken henvender seg til kunden og ber om samtykke til mer informasjon om kjøpspreferanser kan samles inn, slik at butikken kan skreddersy tilbudene til kundens preferanser basert på en kjøpshistorikk eller et spørreskjema som det er frivillig å fylle ut.

- Det gis samtykke til hvert sine formål. Samtykke er gyldig.
- Hvis kunden senere trekker tilbake samtykke, vil han igjen motta de generelle rabattene. Det påfører med andre ord ikke den registrerte noen ulempe eller skade. Samtykke er gyldig.

85

En nettbasert klesforhandler ber i en og samme forespørsel om at kundene godtar at informasjonen deres behandles i forbindelse med levering av kundenes bestilling, og at informasjonen deres brukes til å sende dem markedsføringsmateriell pr. e-post, og i tillegg at informasjonen deres deles med andre selskaper. Samtykke er utformet på en slik måte at kunden enten ikke er enig eller godtar alt.

- Samtykke er ikke detaljert, da det ikke er mulig for kunden å gi separat samtykke for hvert behandlingsformål. I dette tilfellet bør det innhentes eget samtykke for hvert formål. Selskapet bør også vurdere om samtykke er det mest hensiktsmessige grunnlaget for behandling i forhold til levering, eller om det kan være et annet grunnlag for denne behandlingen.

86

En butikk gir sine kunder en samtykkeerklæring, der kunden har mulighet til å krysse av for hvert formål og derved gi samtykke til følgende:
[] Å motta e-post med tilbud om tilbehør til produktet.
[] Å delta i spørreundersøkelser.
[] Å motta påminnelser om service.

- Siden kunden har mulighet til å velge hvilke behandlingsformål som er avtalt, er samtykke frivillig.

87

Ved påmelding ber et treningsstudio kundene om samtykke til å motta et månedlig nyhetsbrev. Senterets eier har også en nettbutikk der han selger treningsapparater. På tidspunktet for registreringen blir kundene også bedt om å gi samtykke til å motta markedsføringsmateriell fra nettbutikken. Samtykkeskjemaet er utformet slik at kunden må krysse av i en rute for å motta nyhetsbrevet og en annen rute for å motta markedsføringsmateriell.

Samtykke i denne situasjonen vil være spesifikk og oppfyller samtidig kravet til oppdeling.

88

En behandlingsansvarlig gir følgende informasjon i forbindelse med anmodningen om samtykke:
* Vi behandler dine personlige data for å forbedre kvaliteten på denne tjenesten.
* I noen tilfeller vil vi videreformidle informasjonen din til tredjeparter for å tilby deg en bedre tjeneste.
* Ved å fortsette å bruke denne tjenesten, samtykker du i behandlingen av dine personopplysninger. Vi samler bl.a. navn, e-postadresse, alder og annen relevant informasjon.
* Denne personopplysningspolicyen kan endres. Besøk nettstedet vårt regelmessig for å holde deg oppdatert.

- Denne informasjonen er av altfor generell art og gir ikke tilstrekkelig spesifikk informasjon om formålet med den tiltenkte behandlingen.

89

En kunde i et kjøpesenter fyller ut et skjema med navn og adresse og legger skjemaet i en glassbolle for å delta i en konkurranse om gratis filmbilletter arrangert av kjøpesenteret. Skjemaet inneholder informasjon om f.eks. formålet med behandlingen. Informasjonen er skrevet i begynnelsen av skjemaet - dvs. før feltene som kunden må fylle ut. Skjemaet er også utformet på en slik måte at kunden må krysse av i en rute for å gi sitt samtykke til at informasjonen skal brukes i trekningen.

- Kundens handling utgjør en klar bekreftelse («utvetydig viljesytring»), som tydelig indikerer en aksept for at kjøpesenteret behandler kundens navn og adresse for å delta i konkurransen.
- Kundens samtykke kan ikke utvides til andre formål, for eksempel at kjøpesenteret kan sende markedsføringsmateriell til kunden.

90

En person fyller ut et elektronisk spørreskjema om sports interesser og sender skjemaet elektronisk.

- Når personen på slutten av spørreskjemaet trykker på "send", vil dette være et uttrykk for vedkommende aksept for at den oppgitte informasjonen kan brukes til de formålene som er angitt i spørreskjemaet, hvis det på forhånd er klart at ved å sende spørreskjemaet, gir samtykke («utvetydig viljesytring»).

91

I forbindelse med bestilling av et ukentlig abonnement på et tidsskrift på nett, presenteres kunden på bestillingssiden med en rute som sier at kunden på tidspunktet for bestillingen også gir sitt samtykke til at utgiveren videreformidler kundens informasjon til andre selskaper i konsernet. Ved siden av boksen er det et allerede huket av i samtykkefelt.

- I eksemplet vil ikke noe gyldig samtykke ha blitt gitt, ettersom det er brukt et forhåndsutfylt kryssfelt, og kunden har dermed ikke gitt et aktivt samtykke.

92

En nettbasert klesbutikk ber om kundens samtykke til å sende e-post med fordelaktige tilbud og rabatter på utvalgte varer når du bestiller. Samtykke gis ved å krysse av i en rute. Det fremgår av informasjonen at kundens samtykke alltid kan tilbakekalles ved å ringe klesbutikken på hverdager mellom 10-16.

- Butikken lever ikke opp til kravet om at det skal være like enkelt å trekke sitt samtykke, som å gi det.

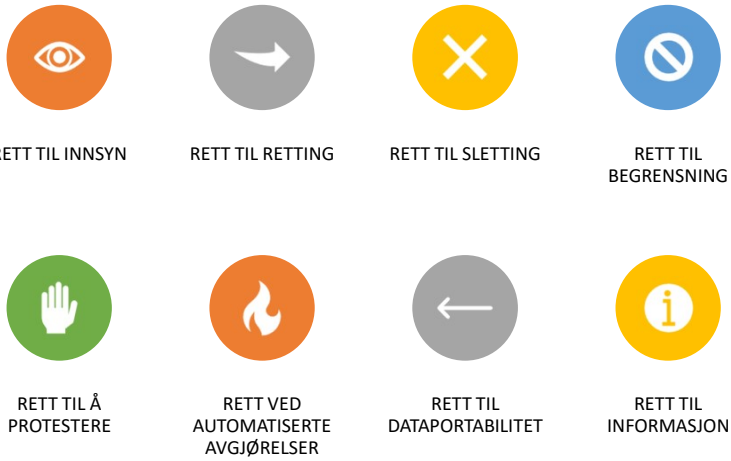
93

Den registrertes rettigheter

Del 7

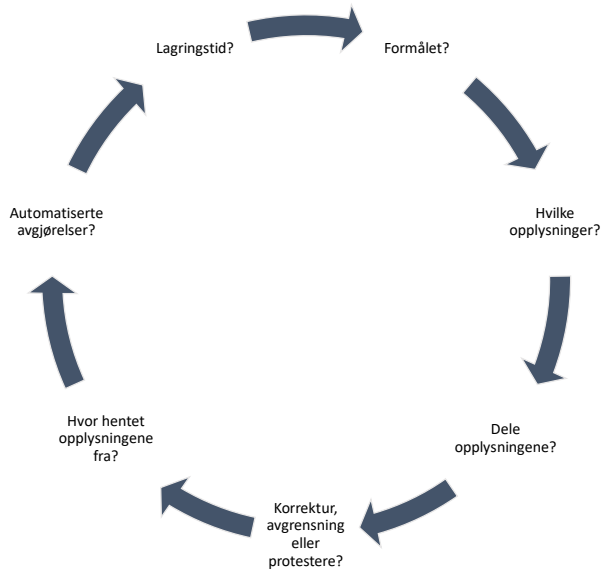
94

Den registrertes rettigheter



95

Artikkel 15. Rett til innsyn



96

Fortale 63 og 64

En registrert bør ha rett til å få innsyn i personopplysninger som er samlet inn om vedkommende, og til på **en enkel måte og med rimelige intervaller å utøve denne retten** for å forvisse seg om og kontrollere at behandlingen er lovlig.

Denne retten bør **ikke ha negativ innvirkning på andres rettigheter** eller friheter , herunder forretningshemmeligheter eller immaterialretten, særlig opphavsretten som programvaren er beskyttet av.

Anmode om at den registrerte **presiserer hvilke opplysninger eller behandlingsaktiviteter anmodningen gjelder**.

Rimelige tiltak for å **kontrollere identiteten** til en registrert som anmoder om innsyn, særlig i forbindelse med nettjenester og nettidentifikatorer.

97

Artikkel 16. Rett til retting

«En virksomhet har forvekslet deg med en annen person. Så snart virksomheten blir oppmerksom på feilen, har den plikt til å rette den.»

98

Er retting mulig?

- Ifølge et saksdokument har noen kommet med en ytring om deg. Ytringen er feilaktig.
- Det er isolert sett korrekt at noen har sagt disse tingene om deg, så du kan ikke kreve at saksdokumentet rettes. Du kan imidlertid kreve å få legge frem tilleggsdokumentasjon som tilbakeviser påstanden.
- Ifølge fastlegens dataprogram tilhører du gruppen med størst sjanse for hjertesykdommer.
- Selv om du aldri får hjertesykdommer, betyr det ikke nødvendigvis at profilen er uriktig, for den uttrykker bare en statistisk sannsynlighet. Du kan imidlertid gå til en annen lege og få en ny vurdering. Denne vurderingen kan supplere fastlegens profil i pasientjournalen din.

99

Artikkel 17. Rett til sletting

- Rett til å bli glemt
- Trekker tilbake samtykket
- Ikke lenger nødvendig
- Innhentet ulovlig
- Sletteplikt etter loven
- Søketreff i søkemotorer

100

Jeg har rett til å få slettet alt dere har på meg!

- Nei, ikke alltid. Man kan f.eks. ikke bare anmode Skatteetaten om å slette det de har registreret på deg.

101

Artikkel 22. Automatiserte individuelle avgjørelser, herunder profilering

- Et dataprogram kan ikke uten videre ta store og viktige avgjørelser om deg hvis:
  - Helautomatisk
  - Juridisk betydning

102

Hva er din rett ved automatiske avgjørelser?

- Dataprogrammet til det offentlige avgjør om du skal få trygd.
  - Du kan kreve at en person ser på avgjørelsen.
- I passkontrollen får du melding om at dataprogrammet synes at du utgjør en stor risiko for landets sikkerhet, og derfor blir du nektet innreise.
  - Du kan kreve at en person ser på avgjørelsen.
- Når du søker om banklån på nett, så avgjør nettstedet lånesøknaden din der og da.
  - Du kan kreve at en person ser på avgjørelsen.
- Persontilpasset markedsføring
  - Generelt ikke nødvendig å kreve sin rett. Årsaken er at slike avgjørelser ikke har stor nok innvirkning på livet ditt.

103

Artikkel 20. Rett til dataportabilitet

- Gjenbruk
- Bytte tjenesteleverandør
- Lesbart filformat
- Krav til samtykke eller kontrakt
- Opplysninger som du selv har oppgitt

104

Artikkel 13 og 14. Rett til informasjon

- Forståelig for målgruppen
- Adskilt fra annen informasjon
- Lett å finne informasjon
- Nødvendig informasjon

105

Hvilken av følgende påstander om retten til begrensning av behandlingen er IKKE riktig?

A. Den registrerte kan be behandlingsansvarlig om å stoppe behandlingen av dataene sine dersom den registrerte bestrider nøyaktigheten av personopplysninger.

B. Den registrerte kan be behandlingsansvarlige om å stoppe behandlingen av dataene sine hvis personopplysninger behandles ulovlig.

C. Den registrerte kan be behandlingsansvarlige om å stoppe behandlingen av dataene sine hvis behandlingsansvarlig ikke lenger trenger personopplysningene i forbindelse med behandlingen.

D. Den registrerte kan be behandlingsansvarlig om å stoppe behandlingen av dataene sine når behandlingen utføres med automatiserte midler.

- D. Den registrerte kan be behandlingsansvarlig om å stoppe behandlingen av dataene sine når behandlingen utføres med automatiserte midler.

106

En virksomhet informerer en kunde om at de kommer til å slette personopplysningene dine siden de ikke lenger er nødvendige. Kan du i henhold til GDPR forhindre sletting av personopplysninger og pålegge begrensningen i bruken i stedet?

A. Ja, ved å trekke tilbake samtykket.
B. Nei, personopplysninger skal slettes når det ikke lenger er nødvendig.
C. Ja, i tilfelle ulovlig behandling.
D. Ja, bare ved å gi en tilleggserklæring.

- C. Ja, i tilfelle ulovlig behandling.

107

kunde ber om å få innsyn i sine opplysninger, kan vi bare henvise til vår personvern

A. Det er tilstrekkelig å henvise til personvernerklæringen.
B. Du kan gi kunden en kopi av personopplysningene mot et rimelig gebyr.
C. Du må gi kunden en gratis kopi av hvorfor og hvordan disse behandles.
D. Du kan gi kunden en kopi hvis personvernombudet gir tillatelse.

- C. Du må gi kunden en gratis kopi av hvorfor og hvordan disse behandles.

108

GDPR krever at man skal ha en personvern-policy på sin hjemmeside, og beskrive hvordan den er utformet

A. Personopplysningsloven stiller krav om ha dette på plass.
B. Personvernforordningen krever ikke spesielt at man skal ha dette.
C. Ikke et krav, men kan være nyttig å ha allikevel.
D. En god personvernpolicy øker den generelle åpenhet om behandlingen.

- C. Ikke et krav, men kan være nyttig å ha allikevel.

109

Hva bør personvernombudet sikre når de mottar forespørsler om sletting av personopplysninger?

A. Sørge for kopier i tilfeller da behandlingsansvarlig krever det
B. Sørge for at kopier oppbevares på kontoret med det høyeste ledernivået
C. Sørge for at kopier relatert til saken oppbevares i en ubestemt periode
D. Sørge for at slettingen er irreversibel og ikke kan gjenopprettes

- D. Sørge for at slettingen er irreversibel og ikke kan gjenopprettes

110

Vurdering av personvernkonsekvenser

Del 8

111

Artikkel 35: Vurdering av personvernkonsekvenser

Dersom det er **sannsynlig** 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.

112

Artikkel 35(3)

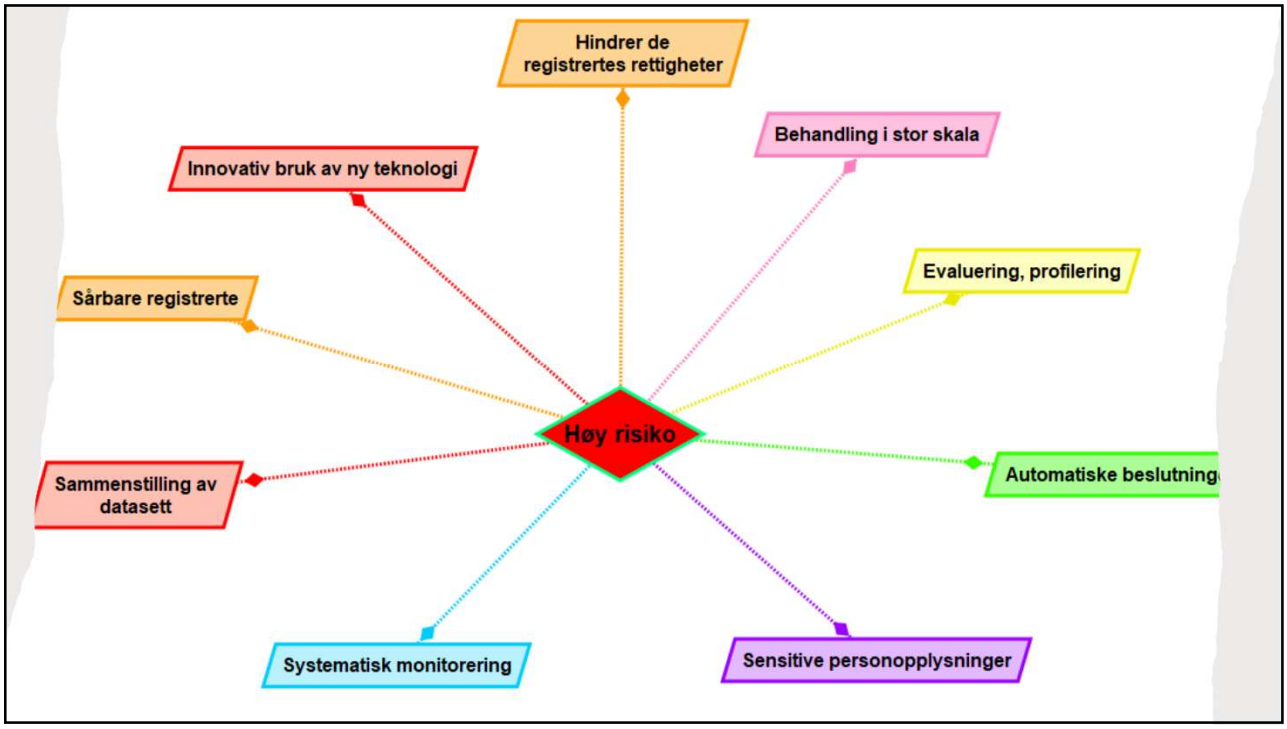
En vurdering av personvernkonsekvenser som nevnt i nr. 1 skal særlig være nødvendig i følgende tilfeller:

a) en 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,

b) behandling i stor **skala av særlige kategorier** av opplysninger som nevnt i artikkel 9 nr. 1, eller av personopplysninger om straffedommer og lovovertredelser som nevnt i artikkel 10, eller

c) en **systematisk overvåking** i stor skala av et offentlig tilgjengelig område

113



114

DPIA - hva er rollen til personvernombudet?

Behandlingsansvarlig er ansvarlig!

Personvernombudet, en uavhengig rolle som gir råd om:

- Er det behov for å utføre
- Hvordan og hvilke metoder bør benyttes
- Kontrollere gjennomføringen
- Bruke interne eller eksterne ressurser
- Hvilke sikkerhetstiltak for å minimere risiko
- Hvorvidt gjennomført på riktig måte
- Er konklusjonene i tråd med regelverket, og kan behandling fortsette

115

Artikkel 35(7)

En systematisk **beskrivelse** av de planlagte behandlingsaktivitetene og formålene med behandlingen, herunder, dersom det er relevant, den berettigede interessen som forfølges av den behandlingsansvarlige,

En vurdering av om behandlingsaktivitetene er **nødvendige** og står i et rimelig forhold til formålene,

En vurdering av **risikoene** for de registrertes rettigheter og friheter som nevnt i nr. 1, og

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

116

I hvilke av de følgende scenariene er det ikke nødvendig med en DPIA?

A. Ny teknologi for å lette behandlingen av personopplysninger i stor skala.
B. Når virksomheten behandler særlige kategorier av personopplysninger.
C. Ved automatisert behandling for evaluering av personlige opplysninger.
D. Det er liten sannsynlighet for høy risiko for personers rettigheter.

- D. Det er liten sannsynlighet for høy risiko for personers rettigheter.

117

Når er en vurdering av personvernkonsekvens er nødvendig?

A. Når behandlingen sannsynligvis ikke vil føre til et høyt risikonivå.
B. Når behandlingen gjelder pasienter til fastlegen.
C. Når det er behandling av sensitive data i stor skala.
D. Når behandlingen er inkludert i den valgfrie listen over aktiviteter.

- C. Når det er behandling av sensitive data i stor skala.

118

Hva er rollen som personvernombud i vurdering av personvernkonsekvenser?

A. Å bestemme hvilke risikoer man skal akseptere
B. Å hjelpe virksomheten med å bestemme om risikoen er akseptabel
C. Å akseptere risikoen
D. Å implementere metoder for aksept av risiko

- B. Å hjelpe virksomheten med å bestemme om risikoen er akseptabel

119

Hva er personvernombudets rolle ved DPIA?

A. Personvernombudet leder DPIA sammen med virksomheten
B. Personvernombudet gir råd til virksomheten når de gjennomfører DPIA
C. Personvernombudet tildeler nødvendige ressurser for å utføre DPIA
D. Personvernombudet bestemmer metodikken som skal følges når de utfører DPIA

- B. Personvernombudet gir råd til virksomheten når de gjennomfører DPIA

120

Veiledninger til DPIA

- https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
- https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/
- https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/
- https://www.cnil.fr/en/PIA-privacy-impact-assessment-en

121

Tilsynsmyndighet

Del 9

122

Datatilsynet

- Opprettet 1980
- Pr. 2020 i underkant av 60 medarbeidere
- Uavhengig forvaltningsorgan under KMD
- To roller – tilsynsorgan og ombud
- Regelverk:
  - Personopplysningsloven
  - Helseregisterloven
  - Helseforskningsloven
  - Politiregisterloven
  - Lov om Schengen informasjonssystem
- Personvernnemnda er klageorgan for våre vedtak

123

Artikkel 58. Myndighet

1. Hver tilsynsmyndighet skal ha følgende undersøkelsesmyndighet:

a) pålegge den behandlingsansvarlige og databehandleren og, dersom det er relevant, disses representant, **å framlegge all informasjon** den trenger for å kunne utføre sine oppgaver,

b) **utføre undersøkelser** i form av personvernrevisjoner,

c) foreta en gjennomgåelse av **sertifiseringer** utstedt i henhold til artikkel 42 nr. 7,

d) underrette den behandlingsansvarlige eller databehandleren om en **påstått overtredelse** av denne forordning,

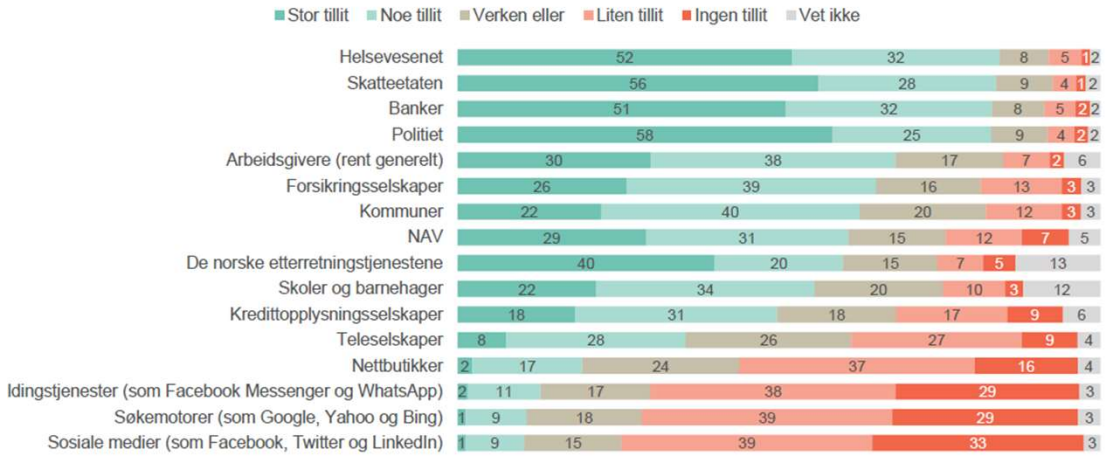
e) få tilgang, fra den behandlingsansvarlige og databehandleren, til **alle personopplysninger** og all informasjon som er nødvendig for å kunne utføre oppgavene den er gitt,

f) **få adgang til alle lokaler** hos den behandlingsansvarlige eller databehandleren, herunder til alt databehandlingsutstyr og -midler, i samsvar med unionsretten eller medlemsstatenes prosessrett

124

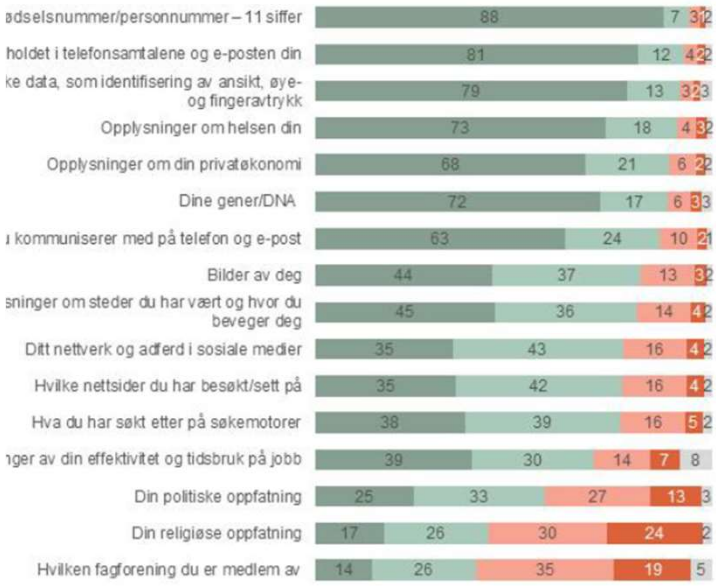
125

Tillit til virksomheters håndtering av personopplysninger (2019)



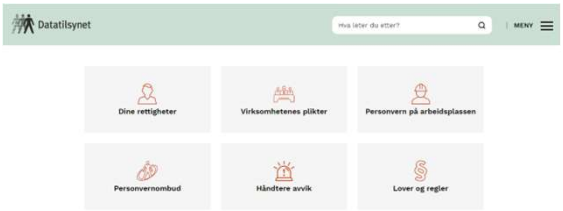
126

Hvilke opplysninger mener du at lovverket særlig bør beskytte mot innsamling og videre bruk? (2019)



127

bestemmer.no
- om personvern, nettvett og digital dømmekraft



Personvernbloggen
Datatilsynets blogg om personvernspørsmål

128

129

Datatilsynets oppgave?

- Telefonsalg og adressert reklame
  - Nei. Såkalt direkte markedsføring, er regulert i markedsføringsloven. Adgangen til å reklamere per sms eller e-post er også regulert der. Markedsføringsloven håndheves av Forbrukertilsynet.
- Nummeropplysningstjenester
  - Nei. Hvis 1881, offentliggjør opplysninger om ditt telefonnummer, adresse og så videre, må du ta kontakt med dem for å reservere deg mot dette.

130

Datatilsynets oppgave?

- Offentliggjøring i pressen
  - Nei. Dersom aviser, blader eller tv skriver om eller publiserer bilder av personer, er dette normalt ikke noe du kan klage inn til Datatilsynet. Dersom du ønsker å klage på pressen, kan du gjøre dette til Pressens faglige utvalg (PFU).

131

Datatilsynets oppgave?

- Privatpersoners behandling av personopplysninger
  - Nei. Personopplysningsloven gjelder som utgangspunkt ikke når privatpersoner behandler personopplysninger for sitt eget private formål. Det betyr for eksempel at de ikke kan bistå i forbindelse med at en privatperson benytter:
    - Kameraovervåkning på egen privat grunn, uten allmenn ferdsel
    - Actionkamera og kameradroner – for eksempel i skibakken
  - Dersom en privatperson publiserer opplysninger om andre på internett, kan personopplysningsloven allikevel gjelde. Da må publiseringen vurderes opp mot ytringsfriheten.

132

Datatilsynets oppgave?

- Brudd på lovbestemt taushetsplikt, fordi det er begrunnet i personvernhensyn.
  - Nei. Det er likevel ikke Datatilsynets sin oppgave å føre kontroll med at taushetsplikt etterleves.
  - Dersom du mistenker brudd på taushetsplikten, kan du henvende deg andre steder:
    - Forvaltningsloven: Du kan ta kontakt med vedkommendes arbeidsgiver, overordnet forvaltningsorgan eller melde saken til politiet.
    - Helseregisterloven eller helsepersonelloven: Du kan ta kontakt med vedkommendes arbeidsgiver, helsetilsynet i ditt fylke eller melde saken til politiet.

133

Datatilsynet har følgende oppgave:

A. Sertifiserer IT – systemer som godkjent som «Privacy-by-design».
B. Tilsyn med alle databehandleravtaler i Norge.
C. Kontrollerer at feilbehandling av personopplysninger blir rettet.
D. Godkjenner leverandører av IT-løsninger med personvern som standard.

- C. Kontrollerer at feilbehandling av personopplysninger blir rettet.

134

Hva er Datatilsynets rolle?

A. Sikre at GDPR blir anvendt på en konsekvent måte
B. Sikre at virksomheter overholder enkeltpersoners rettigheter
C. Å ta bindende avgjørelser i samarbeid med European Data Protection Board
D. Å gi retningslinjer for hvordan man tolker prinsippene i GDPR

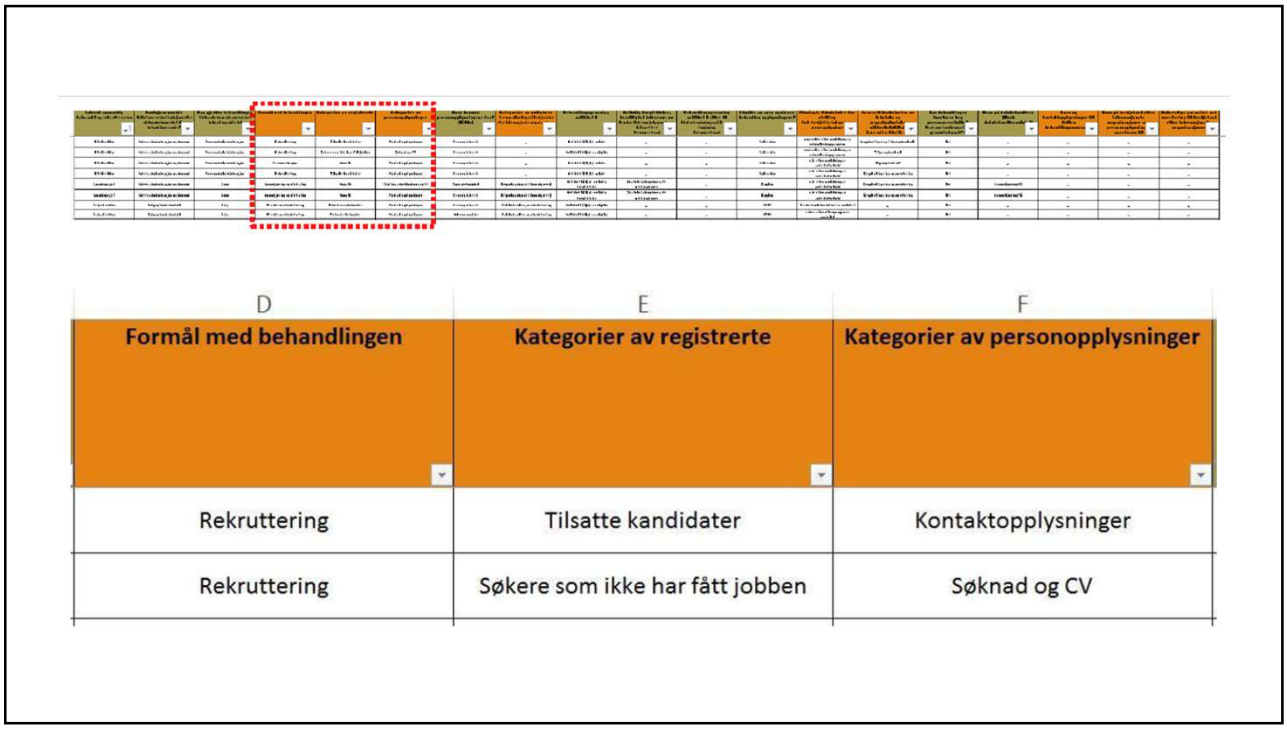
- B. Sikre at virksomheter overholder enkeltpersoners rettigheter

135

Behandlingsprotokoll

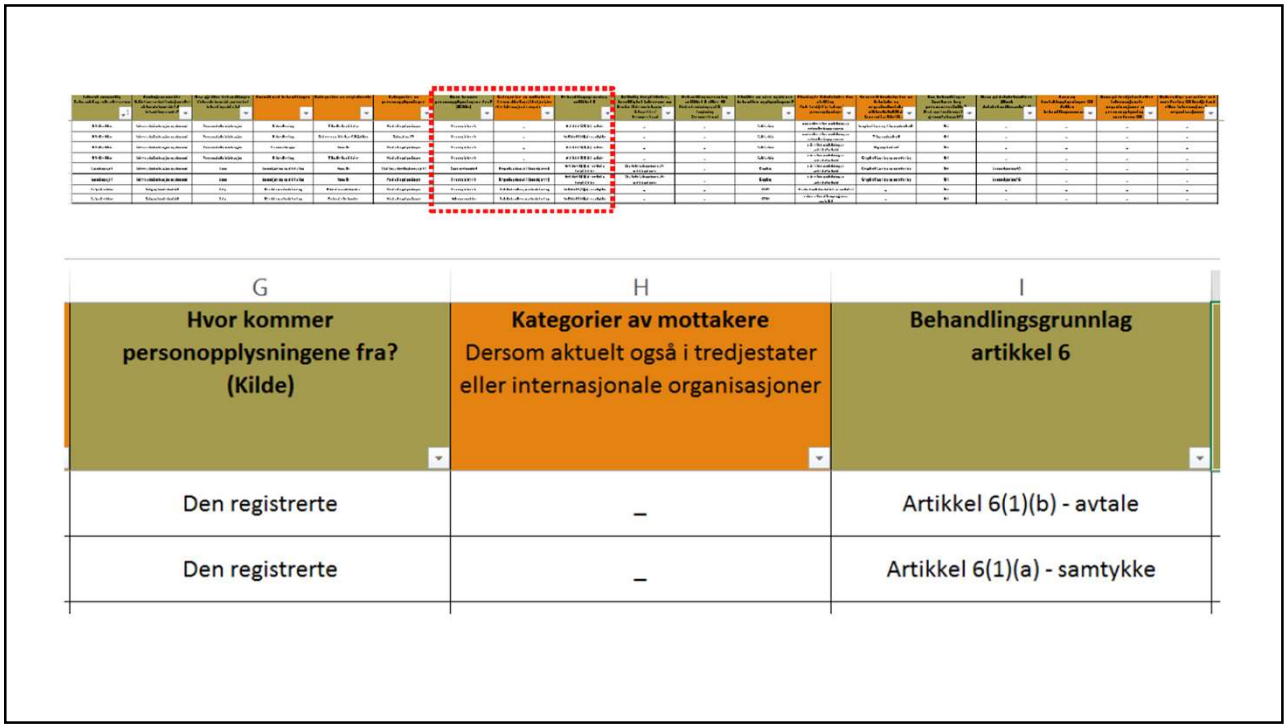
Del 10

136



D	E	F
Formål med behandlingen	**Kategorier av registrerte**	**Kategorier av personopplysninger**
Rekruttering	Tilsatte kandidater	Kontaktopplysninger
Rekruttering	Søkere som ikke har fått jobben	Søknad og CV

137



G	H	I
Hvor kommer personopplysningene fra? (Kilde)	**Kategorier av mottakere** Dersom aktuelt også i tredjestater eller internasjonale organisasjoner	**Behandlingsgrunnlag artikkel 6**
Den registrerte	_	Artikkel 6(1)(b) - avtale
Den registrerte	_	Artikkel 6(1)(a) - samtykke

138

J	K	L
Rettslig forpliktelse, berettighet interesse mv Henvise til dersom beh.grunnlag er 6.1 c,e eller f Dersom relevant	**Behandlingsgrunnlag artikkel 9 eller 10** Med ev henvisning også til annen lovgivning Dersom relevant	**I hvilke av våre systemer behandles opplysningene?**
–	–	Sak/arkiv
–	–	Sak/arkiv

139

M	N	O
Planlagte tidsfrister for sletting Av de forskjellige kategorier av personopplysninger Dersom mulig	**Generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak** Som nevnt i artikkel 32. nr 1 Dersom mulig	**Kan behandlingen innebære høy personvernrisiko?** Blant annet med hensyn til ev gjennomføring av DPIA
x måneder etter avslutning av rekrutteringsprosess	kryptert lagring, tilgangskontroll	Nei
x måneder etter avslutning av rekrutteringsprosess	Tilgangskontroll	Nei

140

Navn på databehandlere (Husk databehandleravtale!) Dersom relevant	Navn og kontaktopplysninger til felles behandlingsansvarlig Dersom relevant	Navn på tredjeland eller internasjonale organisasjoner som personopplysninger overføres til Dersom relevant	Nødvendige garantier ved overføring til tredjeland eller internasjonale organisasjoner Dersom relevant
–	–	–	–
–	–	–	–

141

Databehandleravtale

Del 11

142

Når må man inngå en databehandleravtale?

- Hvis en virksomhet som er behandlingsansvarlig, **setter ut hele eller deler av** behandlingen av personopplysninger til andre virksomheter, er den eller de som behandler opplysningene **på vegne av** den behandlingsansvarlige definert som databehandlere.
- En databehandler kan ikke behandle personopplysninger på en annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige.
- Personopplysningene behandles kun til dine formål.

143

Behandlingsansvarlig - Databehandler
Art. 28.1

Dersom en behandling skal utføres **på vegne av en behandlingsansvarlig**, skal den behandlingsansvarlige **bare** bruke **databehandlere som gir tilstrekkelige garantier** for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen **oppfyller kravene i denne forordning** og vern av den registrertes rettigheter.

144

Behandlingsansvarlig - Databehandler
Art. 28.2

Behandling utført av en databehandler skal være underlagt **en avtale** eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett som **er bindende for databehandleren** med hensyn til den behandlingsansvarlige, og der hensikten med og varigheten av behandlingen, behandlingens formål og art, typen personopplysninger og kategorier av registrerte samt den behandlingsansvarliges rettigheter og plikter er fastsatt.

145

Behandlingsansvarlig - Databehandler
Art. 82.4

Dersom flere enn én behandlingsansvarlig eller databehandler eller både en behandlingsansvarlig og en databehandler er **involvert i samme behandling**, og dersom de i henhold til nr. 2 og 3 er ansvarlige for eventuelle skader som forårsakes av behandlingen, **skal hver behandlingsansvarlig eller databehandles holdes ansvarlig for hele skaden** for å sikre at den registrerte mottar effektiv erstatning.

146

Databehandler - Databehandler Art. 28.2

Databehandleren **skal ikke engasjere** en **annen databehandler** uten at det på forhånd er innhentet særlig *eller* generell **skriftlig tillatelse** til dette fra den behandlingsansvarlige. Dersom det er innhentet en generell skriftlig tillatelse, skal databehandleren underrette den behandlingsansvarlige om eventuelle planer om å benytte andre databehandlere eller skifte ut databehandlere, og dermed gi den behandlingsansvarlige **muligheten til å motsette seg slike endringer**.

147

Databehandler - Databehandler Art. 28.4

Dersom en **databehandler engasjerer en annen databehandler** for å utføre spesifikke behandlingsaktiviteter på vegne av den behandlingsansvarlige, skal nevnte **andre databehandler pålegges de samme forpliktelsene** med hensyn til vern av personopplysninger **som er fastsatt i avtalen** eller i et annet rettslig dokument **mellom den behandlingsansvarlige og databehandleren** som nevnt i nr. 3, ved hjelp av en avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett, der det særlig gis tilstrekkelige garantier for at det vil bli gjennomført tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning. **Dersom nevnte andre databehandler ikke oppfyller sine forpliktelser** med hensyn til vern av personopplysninger, skal **den opprinnelige databehandleren overfor den behandlingsansvarlige ha fullt ansvar for at nevnte andre databehandler oppfyller sine forpliktelser.**

148

Behandlingsansvarlig - Behandlingsansvarlig Art. 26.1

Dersom to eller flere behandlingsansvarlige i **fellesskap fastsetter formålene** med og **midlene** for behandlingen, **skal de være felles behandlingsansvarlige**. De skal på en **gjennomsiktig måte fastsette sitt respektive ansvar** for å overholde forpliktelsene i denne forordning, særlig med hensyn til utøvelse av den registrertes rettigheter og den plikt de har til å framlegge informasjonen nevnt i artikkel 13 og 14 ….

149

Særlig om felles behandlingsansvar

- Hvis to eller flere parter i fellesskap bestemmer, hvorfor det skal behandles personopplysninger (formålet), og hvordan det skal behandles personopplysninger (hjelpemidlene), er de felles behandlingsansvarlige for behandlingen.
- Felles behandlingsansvar kan altså kun komme på tale, hvis du og en eller flere andre parter sammen har ansvaret for en behandling, og hvis dere alle har rett til å bruke opplysningene til egne formål.

150

Databehandleravtale

- Forholdet mellom en behandlingsansvarlig virksomhet og databehandleren skal være **regulert i en databehandleravtale.**
- I **artikkel 28** i personvernforordningen finner man kravene til innholdet i en databehandleravtale.

151

Databehandleravtale?

- Du leier inn en reparatør til å reparere datamaskiner. På datamaskinene kan det ligge personopplysninger.
- Nei. Reparatørens oppdrag går hverken helt eller delvis ut på å behandle personopplysninger. Det foreligger derfor ikke et databehandleroppdrag selv om reparatøren potensielt får tilgang til personopplysninger. Du kan derfor be reparatøren signere en taushetserklæring, men en databehandleravtale er som regel ikke nødvendig.

152

Databehandleravtale?

- Du leier inn en tjeneste som har fjerntilgang til dine systemer. Tjenesten består i å drive support for dine ansatte gjennom systemene. Hovedoppdraget er altså ikke å behandle personopplysninger. Men tjenesten har kontinuerlig fjerntilgang til systemet og personopplysningene som ligger der.
- Sannsynligvis. I dette tilfellet kan man si at oppdraget delvis går ut på å behandle personopplysninger, selv om hovedoppdraget er å yte support. Det foreligger derfor trolig et databehandleroppdrag og man må ha databehandleravtale.

153

Databehandleravtale?

- Du driver en nettbutikk, og bestiller en tjeneste som leverer varene på døra til kundene dine. For at varene skal bli levert til korrekt kunde er det en forutsetning at du må utlevere kundens navn og adresse til leverandøren. Selv om leverandøren mottar personopplysninger er oppdraget å levere varer.
- Nei. Oppdraget er hverken helt eller delvis å behandle personopplysninger. Det foreligger derfor ikke et databehandleroppdrag selv om leverandøren mottar kundens navn og adresse. Leverandøren vil nok her være en selvstendig behandlingsansvarlig for opplysningene han mottar.

154

Databehandleravtale?

- Du er arbeidsgiver og tilbyr dine ansatte å bruke en bedriftshelsetjeneste. De ansatte som ønsker å benytte seg av tilbudet kan melde seg på en liste som virksomheten utleverer til bedriftshelsetjenesten.
- Nei. Oppdraget til bedriftshelsetjenesten er hverken helt eller delvis å behandle personopplysninger på virksomhetens vegne. Oppdraget er å tilby helsetjenester, så for å oppnå dette må bedriftshelsetjenesten motta opplysninger om dine ansatte. Det foreligger derfor trolig ikke et databehandleroppdrag. Bedriftshelsetjenesten vil nok her være en selvstendig behandlingsansvarlig for opplysningene de mottar.

155

Databehandleravtale?

- Virksomheten din benytter revisortjenester.
- Sannsynligvis ikke. Selv om revisoren behandler opplysninger om dine kunder og ansatte har revisoren selvstendige forpliktelser for hvordan opplysningene skal behandles. Videre kan revisoren trolig ikke ta imot detaljerte instrukser fra deg om hvordan opplysningene skal behandles. Dette taler for at det ikke foreligger et databehandleroppdrag.

156

Databehandleravtale?

- Virksomheten din benytter en advokat for å få juridisk rådgivning i en nedbemanningsprosess. Advokaten mottar opplysninger om virksomhetens ansatte for å kunne gi råd.
- Sannsynligvis ikke. Advokaten har selvstendige forpliktelser knyttet til hvordan hun behandler opplysningene, og arbeidsgiver kan derfor ikke alltid instruere advokaten om hvordan hun skal behandle opplysningene. Dette taler for at det ikke foreligger et databehandleroppdrag.

157

Databehandleravtale?

- En skytjeneste tilbyr andre virksomheter å lagre opplysninger i denne. Ansatte hos skytjenesten har i utgangspunktet ikke tilgang til opplysningene i selve skytjenesten, men drifter den og passer på at den er godt nok sikret.
- Ja. Skytjenesten er likevel databehandler da lagringen i skytjenesten i seg selv er behandling av personopplysninger som skytjenesten gjør på vegne av den behandlingsansvarlige.

158

Risikovurdering og interkontroll

Del 12

159

Formålet med internkontroll ivaretatt?

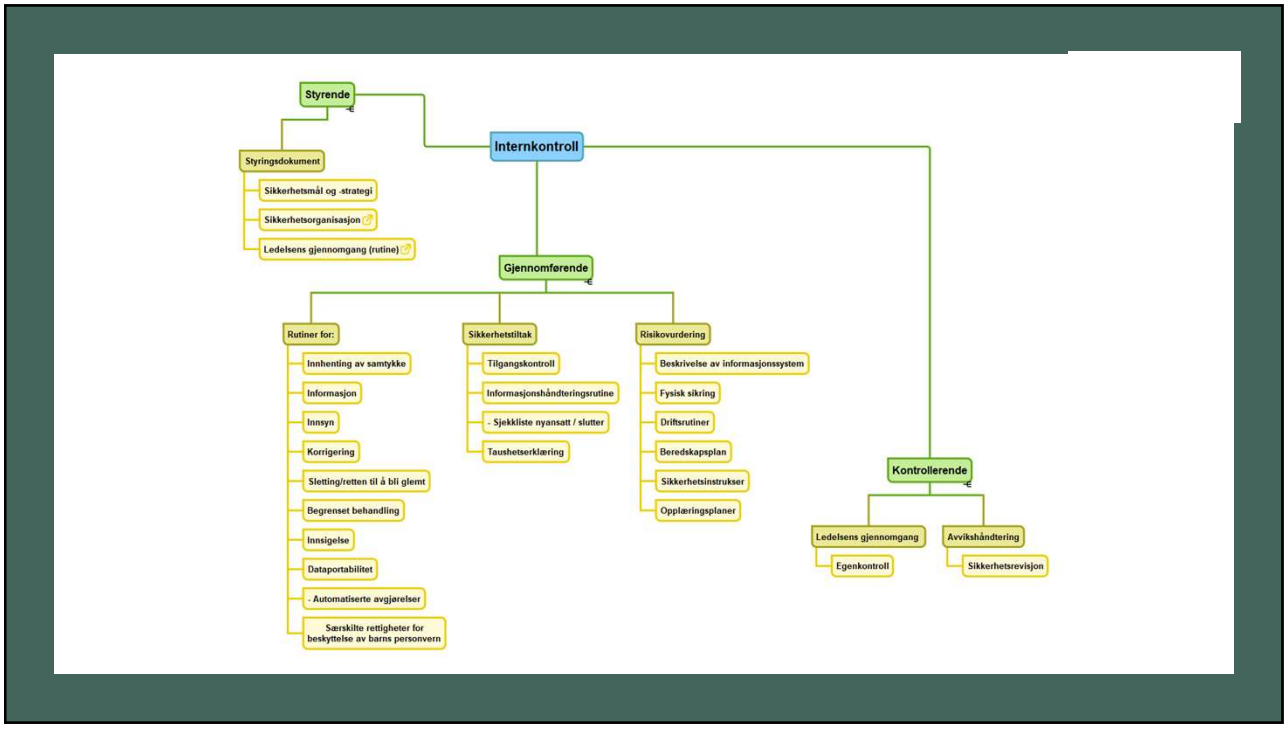
- «Vi har kontroll på vår internkontroll - vi har vurdert virksomhetens risiko i forbindelse med GDPR, for eksempel kostnadene ved å få en bot eller risikoen for å få dårlig omtale i media og miste kunder»
- Nei, for selv om begrunnelsen er forståelig, så er formålet med GDPR å beskytte personopplysninger. Dette betyr at en internkontroll først og fremst er av hensyn til de den registrerte (dvs. personer, ansatte, kunden osv.) - ikke virksomhetens. Dette kan for eksempel være risikoen for at personlig informasjon blir delt med uvedkommende.

160

Hva er internkontroll etter personvernregelverket

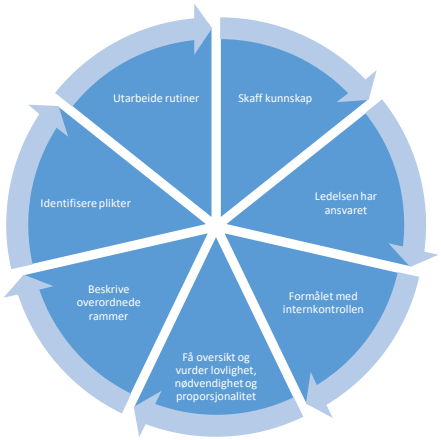
- Sikre en forsvarlig behandling av personopplysninger
  - Sikre den registrertes rettigheter og friheter
  - Ivareta virksomhetens mål med behandlingen
- Ledelsens verktøy for å ivareta sitt ansvar etter lover og regler, og demonstrere etterlevelse
- De ansattes verktøy for å utføre oppgaver på forsvarlig og sikker måte

161



162

Hvordan gjennomføre internkontroll i praksis



163

Risikovurdering

- Formålet er å sikre at den risiko som avdekkes ved behandling av personopplysninger er innenfor det toleransenivå virksomheten har fastlagt.
- Risiko betegner forholdet mellom,
  - sannsynligheten for at en uønsket hendelse vil inntreffe, og
  - konsekvenser av en slik hendelse.
- Virksomheten skal gjennomføre risikovurdering ved endringer i forhold som kan påvirke informasjonssikkerheten, for eksempel,
  - endringer i behandlinger
  - endringer i informasjonssystem
  - endringer i trusselbildet
- Risikovurderingen skal dokumenteres.
- En kontinuerlig prosess – trusselbildet endrer seg i stadig raskere tempo!

164

Definere toleransenivå for risiko (risikoappetitt)

- Toleransenivå for **sikkerhet** defineres enkeltvis for ulike «sikkerhetskategorier»:
  - utilsiktet endring av personopplysninger
  - uautorisert utlevering av personopplysninger
  - manglende tilgjengelighet som kan ha betydning for liv og helse
- Toleransenivå for **personvern** defineres enkeltvis for ulike «personvernscenarier»:
  - at den registrerte ikke lenger har kontroll over sine personopplysninger
  - at den registrerte utsettes for diskriminering på grunn av profilering gjort av programvaren
  - at en person reidentifiseres av opplysninger som er blitt anonymisert

165

Risikovurdering – steg for steg

1. Kartlegging av informasjonsverdier (behandlinger og personopplysninger)
2. Identifiser uønskede hendelser (og årsaker til hendelser)
3. Konsekvensvurdering
4. Sannsynlighetsvurdering (letthet)
5. Vurdering opp mot akseptabel risiko / toleransenivå
6. Tiltak for å redusere risiko

166

Informasjonssikkerhet

- Sikring av **konfidensialitet (K)**
  - informasjon skal ikke bli kjent for uvedkommende
- Sikring av **integritet (I)**
  - informasjon ikke kunne bli endret utilsiktet eller av uvedkommende
- Sikring av **tilgjengelighet (T)**
  - informasjon er tilgjengelig for autoriserte ved behov
- Nytt etter forordningen: **robusthet (R)**
  - organisasjonen og systemene er motstandsdyktige over tid og evner å gjenopprette normaltilstand ved hendelser

KITR er grunnleggende sikkerhetsegenskaper som er en forutsetning for godt personvern.

167

Hendelse	Kategori KITR	Konsekvens	Sannsynlighet	Risiko	Tiltak
Saksbehandler sender sensitive personopplysninger på e-post					
Lege forlater PC med journalsystem pålogget i et område med pasienter					
Ved innføring av nytt saksbehandlingssystem får alle i virksomheten tilgang til alle saker					
Minnepinne med opplysninger om straffbare forhold legges igjen					

168

Konsekvens/sannsynlighet - eksempel på risikomatrise

169

Risikovurdering

Fortale 78: Ved behandling av personopplysninger kreves det at treffes egnede tekniske og organisatoriske tiltak. Det bør derfor **vedtas interne retningslinjer og gjennomføre tiltak.**

170

Oppsummering av regelverket

- Informasjonssikkerhet
  - Artikkel 32, 33, 34
- Internkontroll
  - Artikkel 24, 25, 30
- Databehandlere
  - Artikkel 28, samt eget ansvar i flere artikler
- Andre lover og forskrifter:
  - Helseregisterloven
  - Pasientjournalloven
  - Politiregisterloven
  - Forskrift om Schengen informasjonssystem (SIS-forskriften)

171

Hvordan skal vurderingen av konsekvenser (del av risikovurdering) starte?

- A. Ved å bestemme virkningen av trusler på eiendeler og forretningsvirksomhet
- B. Ved å liste opp virksomhetens ressursbank
- C. Ved å bestemme trusler og sårbarhet
- D. Ved å identifisere relevante risikoer

- D. Ved å identifisere relevante risikoer

172

Hvilke oppgaver har personvernombudet når det gjelder internkontroll?

A. Implementere internkontroll etter en risikovurdering og DPIA.
B. Evaluere personvern og virksomhetens plikter.
C. Overvåke implementeringen av internkontrollen.
D. Velge metode for internkontroll som er relevant for virksomheten.

- C. Overvåke implementeringen av internkontrollen.

173

Hvordan hjelper risikovurdering en virksomhet?

A. Identifisere, rapportere og vurdere uønskede hendelser og risikoen for at disse skal inntreffe
B. Oppdage og rette opp uønskede hendelser etter at de inntraff
C. Korrigere uønskede hendelser etter at de inntraff
D. Behandle kategorier av personopplysninger i stor skala

- A. Identifisere, rapportere og vurdere uønskede hendelser og risikoen for at disse skal inntreffe

174

Hvilke av følgende er ikke oppgaver til personvernombudet i forhold til internkontroll for personvern?

A. Gjennomføre internkontroll på alle behandlingsaktiviteter
B. Gi råd til virksomheten om å følge opp avvik
C. Varsle Datatilsynet om resultatene av internkontroll
D. Forberede virksomheten på andre typer internkontroller

- B. Varsle Datatilsynet om resultatene av internkontroll

175

Personvernombudets oppgaver

Del 13

176

«Det er flere grunner til at virksomheter bør ha et personvernombud:

- *Profesjonalitet*
- *Bygge opp kunnskap internt*
- *Unngå klager fra publikum og ansatte*
- *Slipper meldeplikt til Datatilsynet*

Med et ombud får publikum en fast person å henvende seg til, og det viser at virksomheten tar publikum på alvor!»

(Uttalelse fra Datatilsynet til bladet Kommunal Rapport den 29. januar 2003)

Datatilsynet Kommunal Rapport

177

Viktigste endringer

- Fremhevet og lovregulert
- Skjerpede krav og tydeligere rolle
- Fra frivillig til obligatorisk for mange
- Artikkel 37, 38 og 39 i forordningen
- Retningslinjer fra Personvernrådet (EDPB)

178

Hvem er personvernombud obligatorisk for?

1. Offentlige myndigheter og organer (unntatt domstolene)
2. Behandlingsansvarlige og databehandlere der hovedvirksomheten består av behandlingsaktiviteter som på grunn av sin art, sitt omfang eller formål krever regelmessig og systematisk monitorering i stor skala av registrerte, eller
3. Hovedvirksomheten består av behandling av sensitive personopplysninger i stor skala, eller personopplysninger knyttet til straffbare forhold.

179

Om utpeking av personvernombud

- Både behandlingsansvarlige og databehandlere er omfattet av reglene
- Konserner kan ha felles ombud for underliggende virksomheter og offentlige etater kan oppnevne felles ombud
  - Må være forsvarlig mht tilgang til vedkommende, og mht struktur, størrelse på virksomhetene og omfang og kompleksitet
- Kan kjøpe personvernombud som ekstern tjeneste
- Ikke mer enn ett ombud i én og samme virksomhet

180

Oppgaver

Samle inn og ha oversikt over behandlingsaktiviteter

Involvere seg tidlig, informere og gi råd

Kontrollere overholdelse av personvernregelverket og interne retningslinjer, deriblant ansvarsfordeling, opplæring, holdningsskapende tiltak

Gi råd og delta ved vurdering av personvernkonsekvenser (DPIA)

Være et kontaktpunkt for, og samarbeide med Datatilsynet

Være kontaktpunkt for de registrerte

Skal ha en risikobasert tilnærming til sitt arbeide

Mao: En viktig uavhengig og støttende funksjon for å sikre behandlingsansvarliges etterlevelse av kravene i personvernlovgivningen. Personvernombudet overtar ikke behandlingsansvarliges rolle eller ansvar!

181

Når utpekes et personvernombud?

A. Når behandlingen av personopplysninger blir utført av domstoler.

B. Når kjerneaktivitetene i virksomheten er behandling av særlige kategorier av personopplysninger i liten skala.

C. I tilfeller der en offentlig virksomhet eller organ utfører behandling av personopplysninger, bortsett fra i tilfeller der behandlingen av personopplysninger blir utført av domstoler.

D. Når virksomheten ikke har en juridisk avdeling.

- C. I tilfeller der en offentlig virksomhet eller organ utfører behandling av personopplysninger, bortsett fra i tilfeller der behandlingen av personopplysninger blir utført av domstoler.

182

Hva bør personvernombudet gjøre når han tar beslutninger?

A. Være avhengig av beslutninger fra ledelsen.
B. Rådføre seg med behandlingsansvarlig eller databehandler når han utfører de daglige oppgavene.
C. Rådføre seg med andre ansatte når han tar en beslutning.
D. Være helt uavhengig når han tar beslutninger og utfører de daglige oppgavene.

- D. Være helt uavhengig når han tar beslutninger og utfører de daglige oppgavene.

183

Hvilket av følgende er ikke et ansvar for personvernombudet?

A. Gjennomføre en vurdering av personvernkonsekvenser (DPIA).
B. Gi råd til behandlingsansvarlig eller databehandler i DPIA.
C. Gi råd om ansattes holdning til personvern, og opplæring i så måte.
D. Overvåking av anvendelsen i praksis beskrevet i personvernpolicyen.

- A. Gjennomføre en vurdering av personvernkonsekvenser (DPIA)

184

Hvilket av følgende er ansvaret til personvernombudet?

A. Gi råd til behandlingsansvarlig eller databehandler med hensyn til vurdering av konsekvensene for personvernet og overvåking av tiltak.
B. Implementering av GDPR i virksomheten.
C. Gjennomføre interne revisjoner i virksomheten.
D. Å etablere virksomhetens policy for personvern.

- A. Gi råd til behandlingsansvarlig eller databehandler med hensyn til vurdering av konsekvensene for personvernet og overvåking av tiltak.

185

Basert på Artikkel 39; hvem er det personvernombudet rapporter til?

A. Leder for informasjonssikkerhet
B. Toppledelsen hos behandlingsansvarlig eller databehandler
C. Avdelingsleder
D. Ingen; personvernombudet er uavhengig

- B. Toppledelsen hos behandlingsansvarlig eller databehandler

186

Hvem holdes som ansvarlig i tilfelle brudd på GDPR reglementet?

A. Personvernombudet, hvis registrert hos Datatilsynet
B. Behandlingsansvarlig og databehandler
C. De ansatte som er direkte er involvert i behandling av personopplysninger
D. Informasjonssikkerhetssjef (CISO)

- B. Behandlingsansvarlig og databehandler

187

Hva er rollen som personvernombud i risikovurderingen?

- A. Etablering
- B. Rådgivning og overvåking
- C. Implementere
- D. Testing

- B. Rådgivning og overvåking

188

En liten familiebedrift selger hvitevarer og kjøper tjenester av et webanalysebyrå for å tilby målrettet reklame på nettsiden sin. Er det nødvendig å utpeke et Personvernombud?

- Familiebedriften sin behandling av personopplysninger er såpass begrenset at det ikke faller inn under begrepet «stor skala».
- Webanalysebyrået derimot har så mange forskjellige kunder at dette til sammen tilsvarer behandling av personopplysninger i stor skala. I dette tilfellet skal webanalysebyrået utnevne personvernombud, mens familiebedriften ikke har den samme plikten.

189

Informasjonssikkerhet og personvern som standard

Del 14

190

Fortale 78

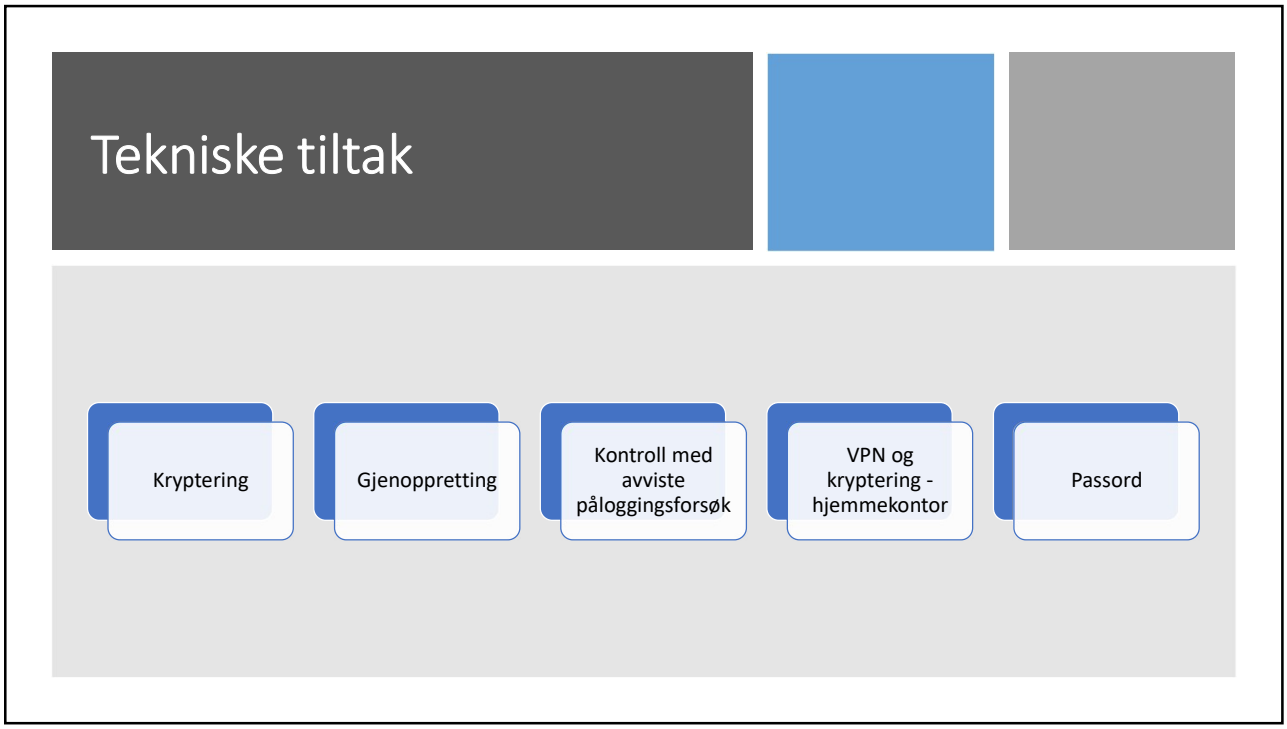
- Ved behandling av personopplysninger kreves det at treffes egnede tekniske og organisatoriske tiltak. Det bør derfor vedtas **interne retningslinjer og gjennomføre tiltak** som særlig overholder prinsippene om **innebygd personvern og personvern som standardinnstilling.**
- Nevnte tiltak kan blant annet omfatte å **minimere** behandlingen av personopplysninger, **pseudonymisere** personopplysninger så raskt som mulig, sikre at behandlingen og formålene med den er åpen, gjøre det mulig for den registrerte å kontrollere behandlingen samt gjøre det mulig for den behandlingsansvarlige å **iverksette sikkerhetsfunksjoner** og å forbedre dem.

191

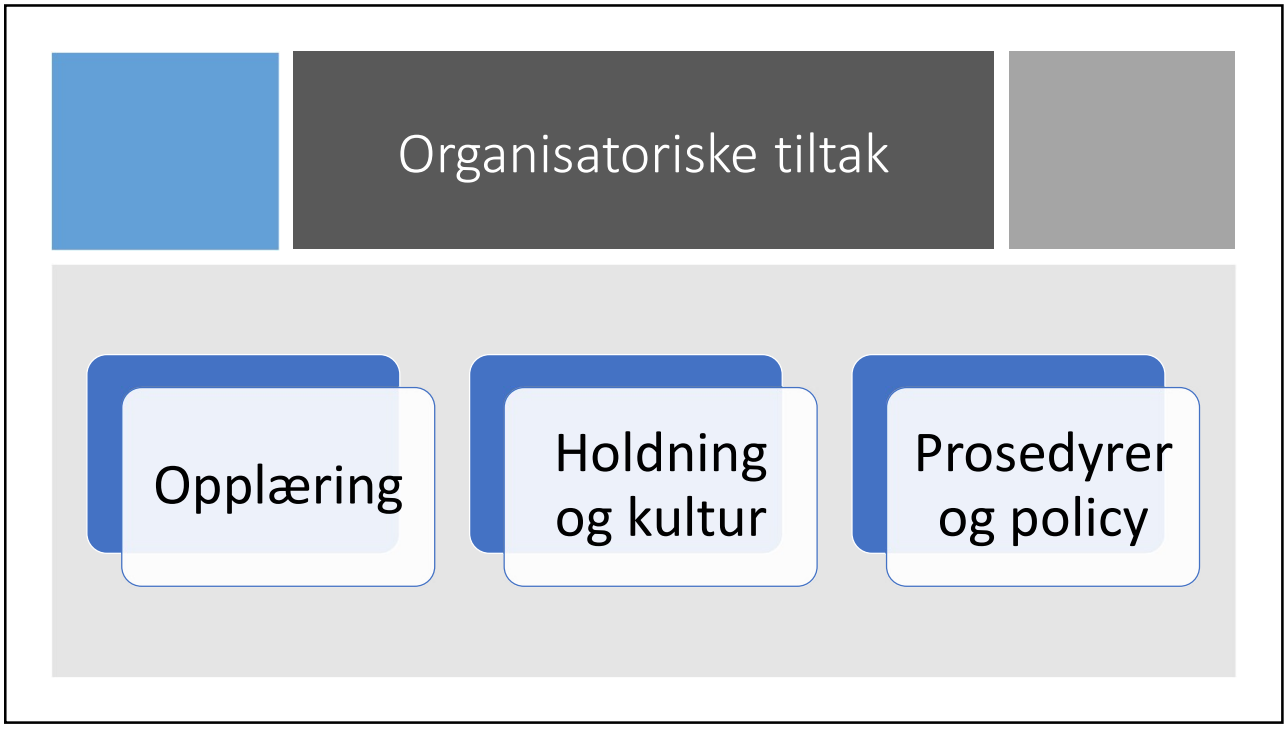
Personvern som standardinnstilling

1. Vær i forkant, forebygg fremfor å reparere
2. Gjør personvern til standardinnstilling
3. Bygg personvern inn i designet
4. Skap full funksjonalitet
5. Ivareta informasjonssikkerheten fra start til slutt
6. Vis åpenhet
7. Respekter brukerens personvern

192


Tekniske tiltak
Kryptering
Gjenoppretting
Kontroll med avviste påloggingsforsøk
VPN og kryptering - hjemmekontor
Passord

193


Organisatoriske tiltak
Opplæring
Holdning og kultur
Prosedyrer og policy

194

Hva er målet med innebygd personvern?

A. Implementere IT-systemer som respekterer personers rettigheter
B. Tiltak som minimerer data gjennom personvennlige innstillinger fra a til å
C. Lage systemer og tjenester som sletter sensitiv informasjon
D. Implementere IT-systemer som verner sensitiv informasjon

- B. Tiltak for dataminimering gjennom personvennlige innstillinger fra a til å

195

Utdyp den innflytelsen GDPR har på nye trender av teknologi som samler inn, lagrer og behandler personopplysninger

- GDPR vil sannsynligvis ha stor innflytelse på ny teknologi som samler inn, lagrer og behandler personopplysninger. Som en konsekvens så må ny teknologi ta i betrakting de høye kravene som stilles i GDPR angående behandling av personopplysninger. De må inkluderes som standard, innebygd personvern, av-identifiseringsmetoder slik som anonymisering og pseudonymisering, og dessuten respekt for de registrerte personenes rettigheter, inkludert retten til å slette, adgang til sine personopplysninger, informasjon om dataportabilitet, og retten til å protestere.
- Helt siden GDPR ble gjeldene , så har de fleste virksomheter (som er underlagt GDPR lovgivningen) begynt på oppgradering til ny teknologi, modifisere plattformens egenskaper for lagring av data og behandling av disse, for å redusere risikoen for mangler i forhold til GDPR. Nye teknologiske lanseringer blir nødt til å ha funksjonalitet for sletting, av-identifisering, og dataminimering. Utviklingen av ny teknologi må ta i betraktning kravene i personvernlovgivningen.
- Teknologi vil på den måten fremskynde tilpasning til GDPR, ved å gjøre det enklere for behandling av personopplysninger, raskere gjenfinning av personopplysninger innen virksomheten, adgangskontroll, automatisering av databehandling, og pseudonymisering og anonymisering.

196

Brudd på personopplysningssikkerheten

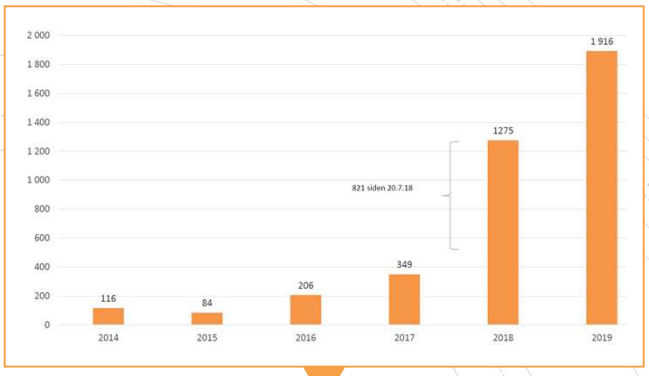
Del 15

197

Frister

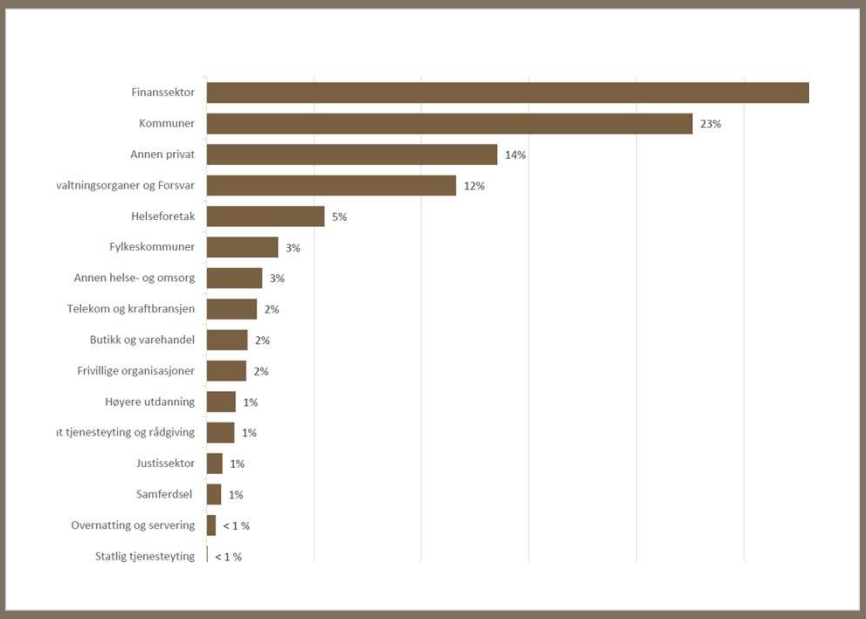
- Avvik skal meldes innen 72 timer etter at man med rimelig grad av visshet har konstatert at det er et brudd på personopplysningssikkerheten
- Databehandler skal melde til behandlingsansvarlig «uten ugrunnet opphold»
- Databehandler kan også melde på vegne av behandlingsansvarlig(e)
- Avvik kan meldes skrittvis, og er i praksis ofte det som skjer

198



Betydelig økning av meldinger om brudd

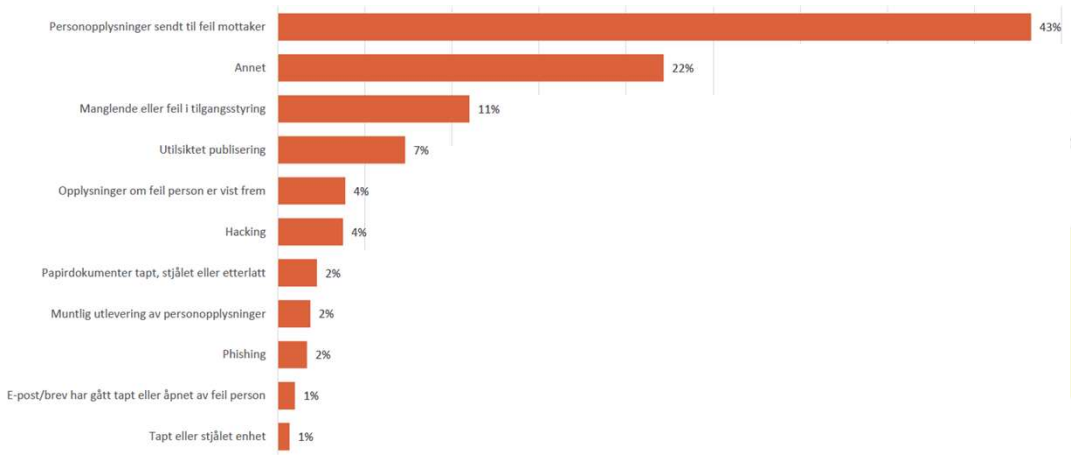
199



Hvem melder flest avvik?

200

Hva slags feil blir meldt



201

Erfaringer

- Feilsending eller annet ved brevpost
- Feilsending av epost
  - Bruk blindkopi ved masseutsendinger
  - Fjern muligheten for autoutfylling av epostadresse
- Publisering på kommunale hjemmesider, postjournal
- Personopplysninger eksponert på læringsplattformer ol (jf Chromebook ol)
- Phishing og hacking
  - Gjennomgang av epostkasser kan bli omfattende med tanke på å identifisere de som kanskje må informeres
  - Bruk to-faktorautentisering også for alminnelige personopplysninger!
- Informasjon til berørte
- «Snokesaker»
- Manglende styring av informasjonssikkerheten, tilgangsstyring, endringer av systemløsninger
- Beskyttede identiteter og hemmelige adresser

202

Informasjon til de berørte

Dersom det er sannsynlig at bruddet vil medføre en høy *risiko…*

- Berørte skal informeres så raskt som mulig, slik at de skal kunne foreta seg noe for å begrense skaden
- Bruk den kanal som det er størst sjanse for å nå ut til den berørte (f.eks. telefon, SMS, e-post, brev)

Unntak i kravet om varsling:

- Eksisterende tiltak som gjør informasjonen uleselig, f.eks. kryptering
- Tiltak i ettertid som sikrer at den høye risikoen ikke lengre vil oppstå
- Uforholdsmessig innsats. Må i stedet informere offentlig eller tilsvarende
- Personopplysningsloven § 16 4. ledd, jf. bokstav a, b og d

203

Når er det høy risiko

- Diskriminering
- Identitetstyveri eller svindel
- Økonomisk tap
- Skade på omdømme

204

Melde avvik

- Hvis vi oppdager et brudd på personopplysningssikkerhete n, løser problemet, og anmelder det til Datatilsynet, så har vi gjort det vi skulle.
- Nei, i mange tilfeller bør man som behandlingsansvarlig også orientere de registrerte – f.eks. kunder, ansatte eller andre opplysninger om personer som kan være kommet i gale hender.

205

En virksomhet har hatt noen brudd på personopplysningssik kerheten innad i finansavdelingen. Basert på GDPR-kravene, hva skal gjøres i dette tilfellet?

A. Hendelsen må rapporteres til alle ansatte i virksomheten senest 72 timer etter at de ble klar over den.
B. Hendelsen må rapporteres til Datatilsynet og de registrerte senest 72 timer etter at han ble klar over den.
C. Hendelsen må rapporteres til Datatilsynet senest 24 timer etter at han ble klar over den.
D. Hendelsen må rapporteres til de registrerte senest 72 timer etter at han ble klar over den.

- B. Hendelsen må rapporteres til Datatilsynet og de registrerte senest 72 timer etter at han ble klar over den.

206

Vi har stanset sikkerhetsbruddet, så det utgjør ikke lengere noen risiko for de registrerte personer.

- Det kommer an på bruddet. Hvis personopplysninger f.eks. har vært eksponeret for uvedkommende, så kan uvedkommende stadig være i besittelse av dem, selv om bruddet er stanset – reelt til evig tid. Risikoen kan derfor bestå, og det kan være krav om å underrette de registrerte.

207

Hva er rollen som personvernombud ved brudd på personopplysnings-sikkerheten?

A. Overvåke og evaluere hendelseshåndtering og responsplan for brudd på personopplysningssikkerheten.
B. Etablere prosedyren for hendelseshåndtering.
C. Håndtere datainnbrudd.
D. Tildele roller og ansvar til personer hendelseshåndtering.

- A. Overvåke og evaluere hendelseshåndtering og responsplan for brudd på personopplysningssikkerheten.

208

I henhold til artikkel 34 i GDPR, hvem skal formidle brudd på personopplysnings sikkerheten til den registrerte og når?

A. Personvernombudet bør informere den registrerte i tilfelle brudd på personopplysninger innen en måned.
B. Personvernombudet skal i alle tilfeller informere den registrerte, til og med når et lite brudd på den registrerte personopplysningene har skjedd.
C. Når bruddet på personopplysninger sannsynligvis vil føre til en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige kommunisere personbruddet til den registrerte uten unødig forsinkelse.
D. Når bruddet på personopplysninger sannsynligvis vil føre til en høy risiko for fysiske personers rettigheter og friheter, skal personvernombudet umiddelbart kommunisere til den registrerte.

- C. Når bruddet på personopplysninger sannsynligvis vil føre til en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige kommunisere personbruddet til den registrerte uten unødig forsinkelse.

209

Overføring av data - utenfor EU EØS

Del 16

210

Overføring av personopplysninger til tredjestater Art. 44

Enhver overføring av personopplysninger som behandles eller skal behandles etter overføring til **en tredjestat** eller til en internasjonal organisasjon, skal finne sted **bare dersom** den behandlingsansvarlige og databehandleren, med forbehold for de andre bestemmelsene i denne forordning, **oppfyller vilkårene i dette kapittel**, herunder for videreoverføring av personopplysninger fra tredjestaten eller en internasjonal organisasjon til en annen tredjestat eller en annen internasjonal organisasjon. **Alle bestemmelser i dette kapittel skal få anvendelse for å sikre at det nivået for vern av fysiske personer som garanteres i denne forordning, ikke undergraves.**

211

(Art. 45) Tilstrekkelig beskyttelse

European Commission

Personopplysninger kan overføres til en tredjestat eller en internasjonal organisasjon når **Kommisjonen** har fastslått at tredjestaten, et territorium eller en eller flere angitte sektorer i nevnte tredjestat eller den aktuelle internasjonale organisasjonen **sikrer et tilstrekkelig beskyttelsesnivå**.

212

Tilstrekkelig beskyttelse

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Japan, New Zealand, Switzerland, Uruguay ~~and the United States of America (limited to the Privacy Shield framework)~~ as providing adequate protection.

Standardiserte avtalevilkår - lagd av Kommisjonen: link

213

214

Nødvendige garantier
Art. 46

Dersom det ikke foreligger en beslutning i henhold til artikkel 45 nr. 3, **kan** en behandlingsansvarlig eller databehandler overføre personopplysninger til en tredjestat eller en internasjonal organisasjon **bare dersom den behandlingsansvarlige eller databehandleren har gitt nødvendige garantier,** og under forutsetning av at de registrerte **har håndhevbare rettigheter og effektive rettsmidler.**

215

Unntak
Art. 49

- uttrykkelig gitt samtykke
- informert om de mulige risikoene
- nødvendig for å oppfylle en avtale
- hensyn til viktige samfunnsinteresser,
- forsvare rettskrav

216

Kursleverandøren har redusert kostnadene ved å lagre kursdeltakere hos ekstern leverandør i Kina. Hva må kursleverandøren sørge for?

- Databehandleravtale art. 28 nr. 3 bokstav a-h.
- Bakgrunnssjekk.
- Garantier for at forpliktelser i GDPR blir overholdt.
- Eu's klausuler.
- Må dokumentere.
- Sjekke at de kan håndheves i Kina.

217

Kursleverandøren har avdelinger i flere land i Europa og USA. All lagring og fakturering av kursdeltakere skjer hos hos datterselskap i Tyskland. Kursleverandøren inngikk nylig en avtale med TwoDrive, som skal lagre deler av opplysningene som behandles av datterselskap i Tyskland. Hvilke konkrete tiltak må tas for å sikre lovligheten av disse overføringene?

- Kursleverandør er behandlingsansvarlig. Datterselskap i Tyskland er databehandler. TwoDrive er en underdatabehandler og må signere en databehandleravtale med samme forpliktelser som for datterselskapet.
- Det bør velge mellom standardiserte klausuler eller (kanskje) bindende selskapsregler.

218