
KVALE
ADVOKATFIRMA

Hvilke krav stiller personvernforordningen (GDPR) til din virksomhet?

ALSO - webinar

7. februar 2018

Jens Christian Gjesti

Dagens opplegg

I. Hva er personvernforordningen?

II. Hvordan går du frem for å oppfylle kravene i tide?

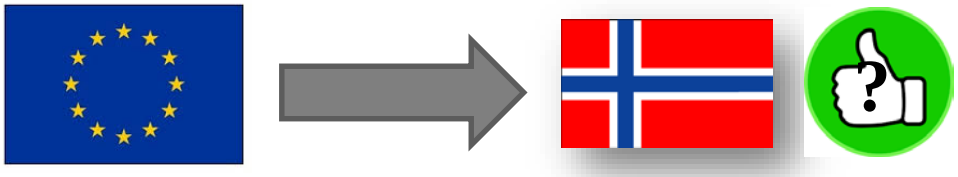
III. Hvilke grunnleggende krav stiller den til min virksomhet?

IV. Hva må jeg tenke på som a) "behandlingsansvarlig" og b) "databehandler"?

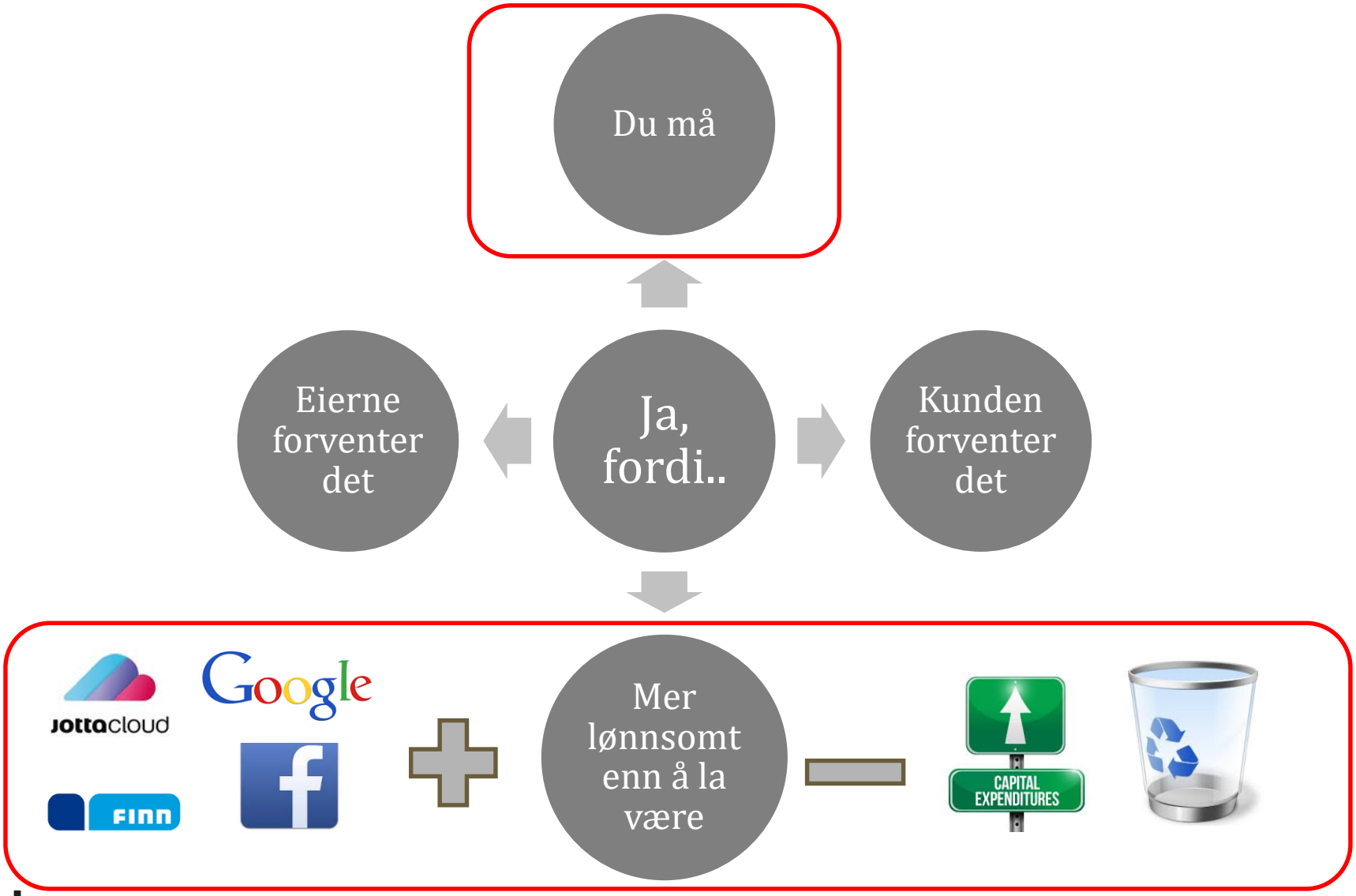
V. Hvilke rettigheter har "de registrerte"?

Hva trenger du å vite om personvernforordningen?

1. Hva?	• Modernisering av dagens personvernregler • Populært kalt "GDPR"
2. Hvorfor?	• Styrke rettigheter i en digital verden (1995 - 2017) • Økt forutsigbarhet for næringslivet
3. Hvordan?	• EU-forordning som norsk lov • ..supplert med nasjonale tilpasninger (CCTV mv.)
4. Når?	• Justis- og beredskapsdepartementet: "Norge skal implementere reglene **25. mai 2018**



Hvorfor skal dere bry dere om personvernforordningen?



Hvorfor skal dere bry dere om personvernforordningen? (2)

— Systemet skal brukes, men det er **ikke sånn at bøter skal være de mest vanlige måtene å håndtere lovbrudd på**, sier Bjørn Erik Thon, som er direktør i Datatilsynet.

Dagens opplegg

I. Hva er personvernforordningen?

II. Hvordan går du frem for å oppfylle kravene i tide?

III. Hvilke grunnleggende krav stiller den til min virksomhet?

IV. Hva må jeg tenke på som a) "behandlingsansvarlig" og b) "databehandler"?

V. Hvilke rettigheter har "de registrerte"?

Hva skal virksomheten være innen 25. mai 2018?

Krav

- **Grunnleggende personvernprinsipper**
- **Krav til deg som "behandlingsansvarlig"**
- **Krav til deg som "databehandler"**
- **Krav til deg som følge av "de registrertes rettigheter"**
- **Annet (overføring til utlandet mv.)**

Leveranse

A) Dokumentasjon
- Oversikt/protokoll
- Internkontroll
- Informasjonssikkerhet
- DPIA
- Databehandleravtaler
- Personvernpolicy mv.

B) Organisatoriske tiltak
- Personvernrutiner
- Sikkerhetsrutiner
- Personvernombud
- Rolle-/ansvarsfordeling
- Mv.

C) Tekniske tiltak
- Logiske sikkerhetstiltak
- Fysiske sikkerhetstiltak
- Teknisk støtte for innsyn, dataportabilitet, sletting
- Mv.

Hvor er virksomheten per i dag?

Krav

- **Grunnleggende personvernprinsipper**
- **Krav til virksomheten som "behandlingsansvarlig"**
- **Krav til virksomheten som "databehandler"**
- **Krav som følge av "de registrertes rettigheter"**
- **Annet (overføring til utlandet mv.)**

Leveranse

A) Dokumentasjon

- Oversikt/protokoll
- Internkontroll
- Informasjonssikkerhet
- DPIA
- Databehandleravtaler
- Personvernpolicy mv.

?

B) Organisatoriske tiltak

- Personvernrutiner
- Sikkerhetsrutiner
- Personvernombud
- Rolle-/ansvarsfordeling
- Mv.

?

C) Tekniske tiltak

- Logiske sikkerhetstiltak
- Fysiske sikkerhetstiltak
- Teknisk støtte for innsyn, dataportabilitet, sletting
- Mv.

?

Hvordan skal dere klare å oppfylle de nye kravene i tide?

Nye personvernregler fra 2018. Hva betyr det for din virksomhet?

Hva blir nytt?

1 Alle norske virksomheter får nye plikter
Alle virksomheter må sette seg inn i den nye lovgivningen og finne ut hvilke nye plikter som gjelder dem. Ledelsen må sørge for å få på plass rutiner for å overholde de nye pliktene. Alle ansatte må følge de nye rutinene når reglene trer i kraft.

2 Alle skal ha en forståelig personvernerklæring
Informasjon om hvordan din virksomhet behandler personopplysninger skal være lett tilgjengelig og skrevet på en forståelig måte. Det nye lovverket stiller strengere krav til informasjonens form og innhold enn dagens lovgivning. All informasjon som gis til barn, skal tilpasses barnas forståelsesnivå.

3 Alle skal vurdere risiko og personvernkonsekvenser
Dersom et tiltak utgjør en stor risiko for personvernet, må virksomheten også utrede hvilke personvernkonsekvenser det kan ha. Hvis utredningen viser at risikoen er stor og dere selv ikke kan redusere den, skal Datatilsynet involveres i forhåndsdrøftelser.

4 Alle skal bygge personvern inn i nye løsninger
De nye reglene stiller krav til at nye tiltak og systemer skal utarbeides på en mest mulig personvernvennlig måte. Dette kalles innebygd personvern. Den mest personvernvennlige innstillingen skal være standard i alle systemer.

5 Mange virksomheter må opprette personvernombud
Alle offentlige og mange private virksomheter skal opprette personvernombud. Et personvernombud er virksomhetens personvernekspert, og et bindeledd mellom ledelsen, de registrerte og Datatilsynet. Ombudet kan være en ansatt eller en profesjonell tredjepart.

6 Reglene gjelder også virksomheter utenfor Europa
Virksomheter som holder til utenfor Europa må også følge forordningen, dersom de tilbyr varer eller tjenester til borgere i et EU- eller EØS-land. Dette gjelder også om de ikke direkte tilbyr tjenester, men kartlegger adferden til europeiske borgere på nett. De som er etablert i flere land i Europa, skal bare trenge å snakke med personvernmyndighetene i det landet der de har sitt europeiske hovedkvarter.

7 Alle databehandlere får nye plikter
Databehandlere er virksomheter som behandler personopplysninger på oppdrag fra den ansvarlige virksomheten. Ofte er det snakk om leverandører av IT-tjenester. De nye reglene pålegger databehandlere å ha rutiner for innsamling og bruk av personopplysninger. Databehandlere skal også si ifra til oppdragsgiveren sin hvis de får instrukser som er i strid med loven. Oppdragsgiver skal også godkjenne databehandlerens underleverandører. Databehandlere kan også bli holdt økonomisk ansvarlig sammen med oppdragsgiver.

8 Alle bør samarbeide i egne nettverk og følge bransjenormer
De nye reglene oppmuntrer til sektorvis utforming av retningslinjer og bransjenormer. Om dere følger bransjenormer, vil dere ha de viktigste rutinene på plass. Datatilsynet skal godkjenne bransjenormene.

9 Alle får nye krav til avvikshåndtering
Reglene for håndtering av sikkerhetsbrudd blir strengere. Forordningen stiller krav til når det skal varsles, hva varselet skal inneholde og hvem som skal varsles. Kort sagt skal man si fra raskere og oftere enn man gjør i dag.

10 Alle må kunne oppfylle borgernes nye rettigheter
Den enkeltes rett til å kreve at hans eller hennes personopplysninger slettes blir styrket. Dette kalles «retten til å bli glemt». Norske og europeiske borgere vil blant annet kunne kreve å ta med seg personopplysningene sine fra en leverandør til en annen i et vanlig brukt filformat. Dette kalles «dataportabilitet». De kan også motsette seg profilering. Alle henvendelser fra borgere skal besvares innen en måned.

Hva bør dere gjøre nå?

1 Ha oversikt over hvilke personopplysninger dere behandler
Alle virksomheter som samler inn eller bruker personopplysninger skal ha oversikt over hvilke personopplysninger det er snakk om, hvor de kommer fra og hva som er det rettslige grunnlaget for behandlingen. Sørg for å ha en slik oversikt. Det er et krav som gjelder også etter dagens lov.

2 Sørg for å oppfylle dagens lovkrav
Overgangen til de nye reglene blir lettere om dere etterlever kravene i personopplysningsloven, som gjelder i Norge i dag. Har dere gode rutiner for internkontroll som fungerer etter hensikten og er kjent i organisasjonen, er det lettere å få oversikt over hva dere må endre.

3 Sett dere inn i det nye regelverket
Dere finner forordningsteksten på Datatilsynets nettsider. Der fyller vi også på med artikler om de nye reglene etter hvert som vi utarbeider dem.

4 Lag rutiner for å følge de nye reglene
Gå gjennom rutinene dere har for behandling av personopplysninger. Oppdater dem etter nytt regelverk der det trengs. Dokumenter de nye rutinene, og legg en plan for nødvendige endringer. Er systemene deres laget for å ivareta kravet til innebygd personvern, dataportabilitet og personvern som standardinnstilling? Klarer dere å fange opp og besvare henvendelser fra borgerne innen én måned? Endringer i systemer og rutiner tar tid. Begynn allerede nå!

datatilsynet.no/forordning

1. Få oversikt

2. Oppfylle dagens krav

3. Forstå nye krav

4. Legg en plan

– Vi oppfordrer norske virksomheter til først og fremst å **gå igjennom systemene sine og se om de oppfyller dagens lovkrav**. Selv om det kommer et nytt regelverk, må de fortsatt forholde seg til det gamle frem til mai 2018. Det er mye nytt, men ikke alt.

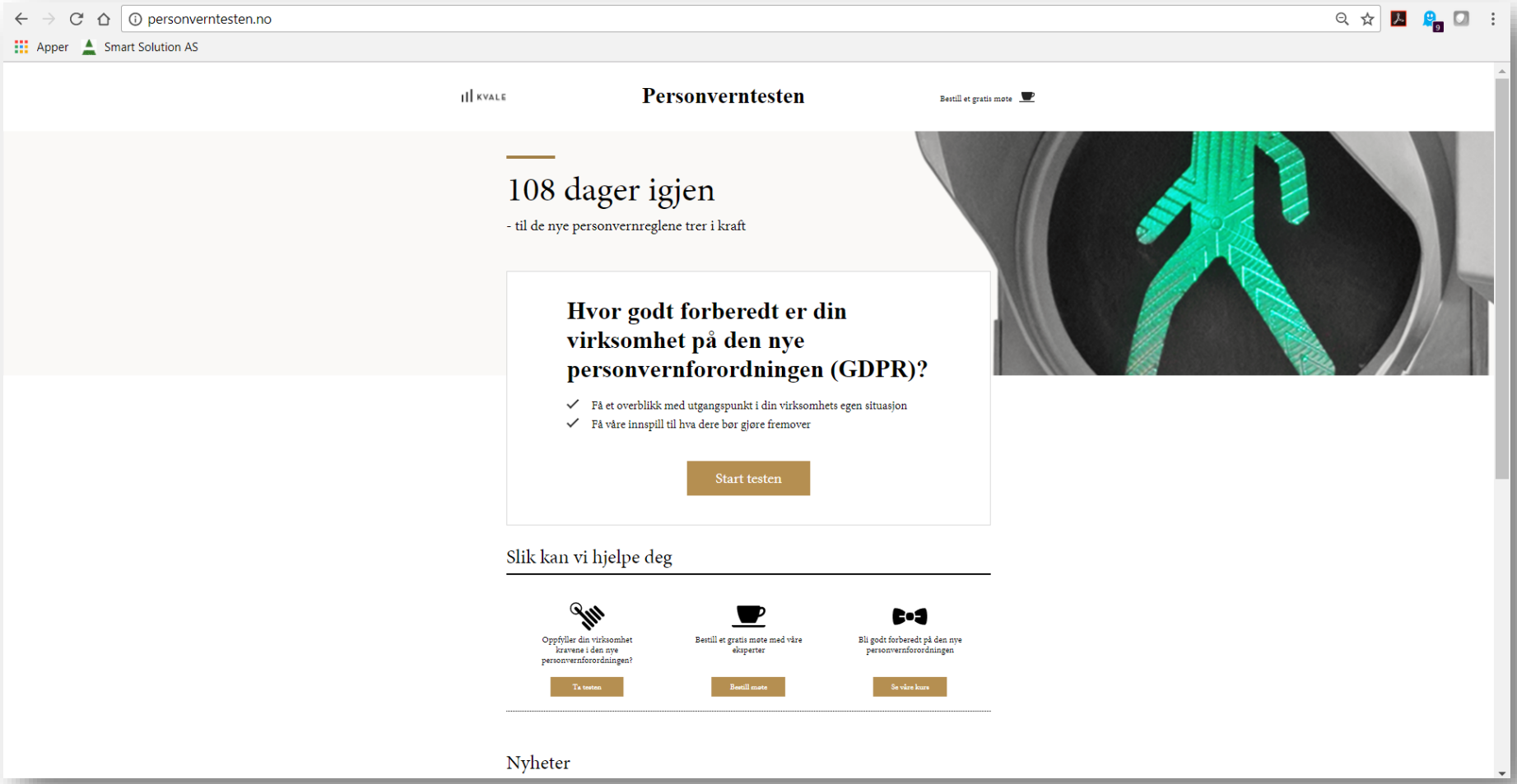
Trude Talberg-Furulund, seniorrådgiver i Datatilsynet

KVALE

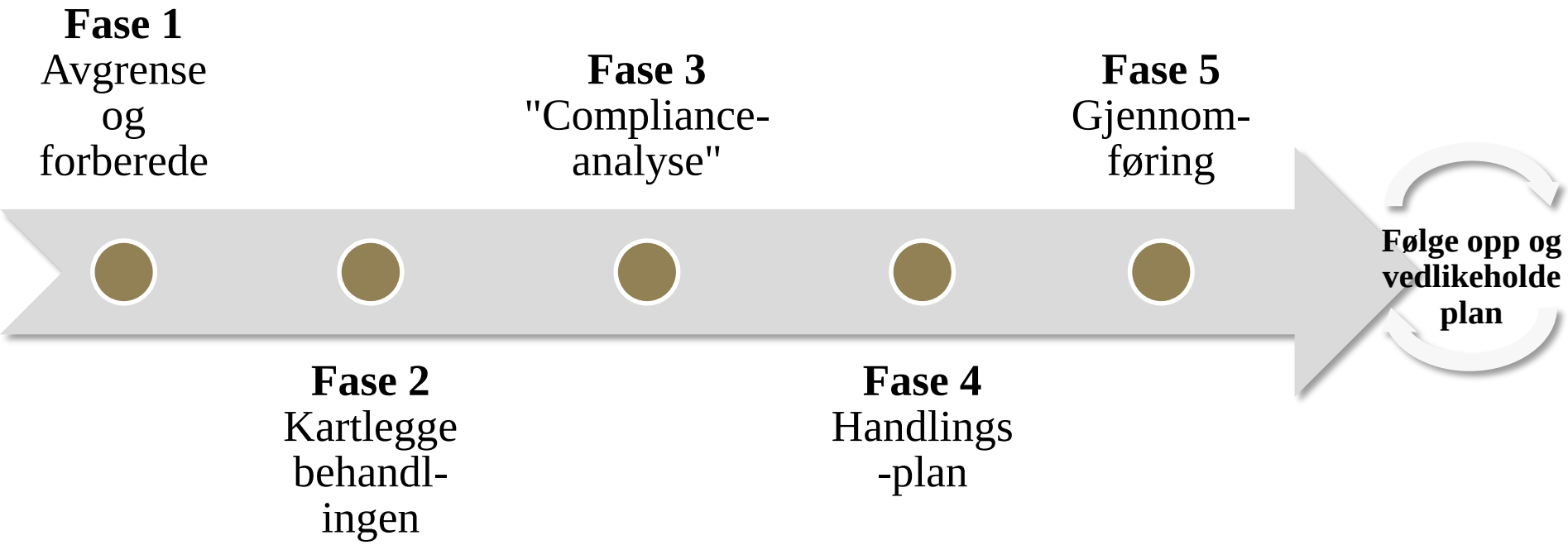
https://datatilsynet.no/globalassets/global/05_regelverk/forordningen/punkter_ny-forordning_web_1.pdf

Hvordan får dere oversikt over hvordan dere ligger an?

www.personverntesten.no



Hvordan kan du organisere prosjektet?

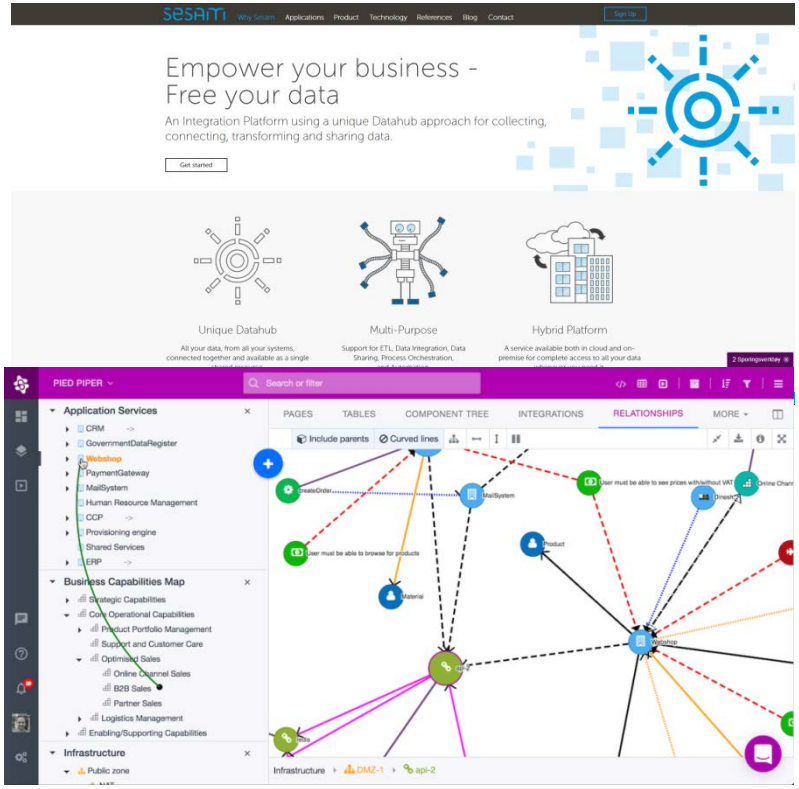


Hvordan går du frem for å komme dit innen fristen?

IT-funksjonalitet

vs.

Manuell kartlegging/implementering



Eksempel på oversikt over personopplysninger som behandles

Informasjon Formål	Behandlings-grunnlag	Melding/ Konsesjon	Sensitive person-opplysninger	Sikkerhets-tiltak	Lagring og kommunikasjon	Opplysningenes omfang	Avdeling	System-/ dataeier
Lønn og personal: - lønnsopplys-ninger - personal-opplysninger	Personopplys-ningsloven, § 8f	Unntatt i forskriftens § 7–16	Nei			Ca. 130 ansatte		
Barnevern: - vurdering og tiltak	Barnevern-loven, § 3-1	Meldt 14.01.2009	Ja			Ca. 68 barn og foresatte		
Helseopplys-ninger: - pasient-journal	Helseper-sonelloven § 39 flg.	Meldt 14.01.2009	Ja			Ca. 413 pasienter		
Elevadminis-trasjon - elever / foresatte - lærere	Opplærings-loven § 13-5		Ja			Ca. 219 søkere		
Hendelses-register: - logg over brudd	Personopplys-ningsloven, § 13	Unntatt i forskriftens § 7–11	Nei			Arkivlogg, nettverks-logg og serverlogg, PC-logger		
Kunde-opplysninger - Salgskontakter - Leveranse-kontakter	Personopplys-ningsloven, § 8 a		Nei			Ca. 8000		

MER SPESIFIKT SKAL OVERSIKTEN GI KORTFATTET INFORMASJON OM

- hvilke opplysninger som behandles og formålet med behandlingen
- hjemmelsgrunnlag for å behandle opplysningene
- klassifikasjon av hvorvidt personopplysningene er

EKSEMPEL PÅ FREMGANGSMÅTE FOR KARTLEGGING AV BEHANDLINGER:

1. Dersom kartleggingen gjelder en større virksomhet, kan sikkerhetsansvarlig eller prosjektleder sende ut forespørsel om behandling av personopplysninger til hver avdelings-leder: Hva behandles, lagres eller overføres?

https://www.datatilsynet.no/regelverk-og-skjema/veiledere/internkontroll_informasjonssikkerhet/

KVALE

Dagens opplegg

I. Hva er personvernforordningen?

II. Hvordan går du frem for å oppfylle kravene i tide?

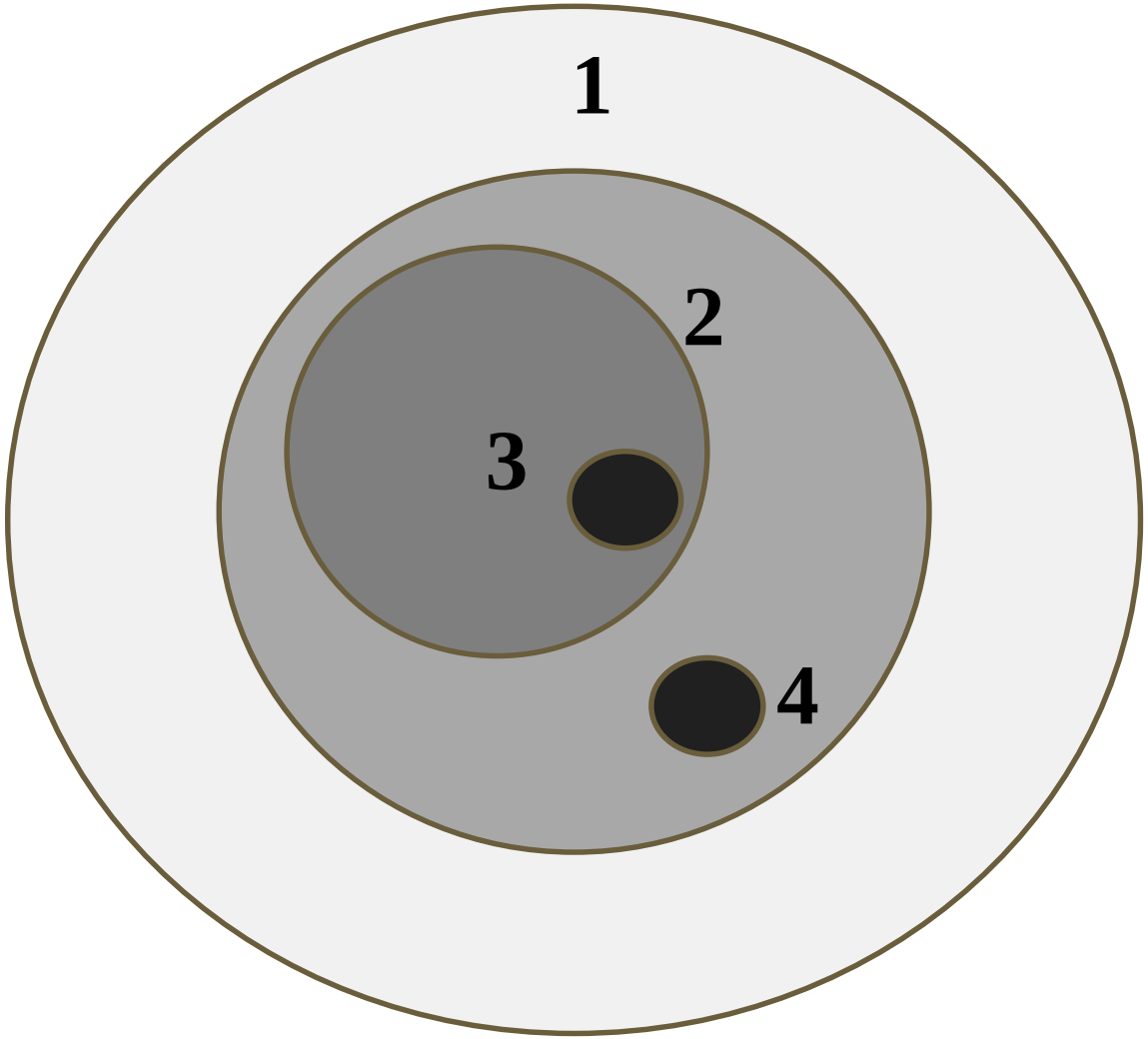
III. Hvilke grunnleggende krav stiller den til min virksomhet?

IV. Hva må jeg tenke på som a) "behandlingsansvarlig" og b) "databehandler"?

V. Hvilke rettigheter har "de registrerte"?

Når gjelder de nye reglene for deg?

1. **Rådata**
2. **Personopplysninger**
3. **Personopplysninger med behandlingsgrunnlag**
4. **Spesielle kategorier/sensitive personopplysninger**



Hvilke personopplysninger behandlere dere i din virksomhet?

Indirekte – eks. adresse, telefonnummer, IP-adresse, adferdsmønster, "location data", "online identifiers", "factors specific to the physical, economic, cultural or social identify of that person"

Direkte – eks. navn, fødselsnummer, bilde, ansattnummer, irismønster

Personopplysning - "opplysninger og vurderinger som kan knyttes til en enkeltperson"

KVALE

Vil dine data være personopplysninger?

Kundebase	• Navn, adresse, kjønn, fødselsnummer, fakturadato, abonnement, dialog med kundeservice, opptak mv. ✓
Informasjon om transaksjoner	• Vare/tjeneste, dato, sum, antall kjøp, betalingsmåte, reklamasjoner mv. ✓
Metadata	• IP-adresse, MAC-adresse, telefonnr., tidspunkt, lengde, type tjeneste, lokasjon, CDR, mv. ✓
Analyse/"profilering" av kunden	• Bruksmønster, kredittrisiko, risikoprofil, livsstil, helsetilstand, vaner, mottagelighet for reklame mv. ✓

Er du i tvil? Behandle data som om de er personopplysninger

Vil dere ha lov til å "behandle" dataene?

A) Grunnlag i lov/forskrift?

- Eks. regnskap, hvitvasking, arbeidsmiljøloven

B) Nødvendig for å..

- oppfylle avtale med den registrerte?
- ivareta berettiget interesse?

C) Eller samtykke?

- "Frivillig"
- "Informert"
- "Uttrykkelig"
- "Utvetydig"

Behandlingsgrunnlag for kundedata?

All bruk av personopplysninger er regulert ("behandling")

Hvordan skriver du et samtykke?

KRAV:
- ✓ Aktivt og informert
- ✓ Adskilt fra annen tekst
- ✓ Ikke betingelse
- ✓ Kan trekkes tilbake
- ✓ Enkelt og forståelig språk

☐ **"Jeg samtykker til at jeg forstår hva dere ber meg om å samtykke til, hva dere skal bruke mine personopplysninger til og hvordan, hvem dere deler dem med, hvordan jeg kan rette og slette mine opplysninger, og hvor lenge dere oppbevarer dem. Dersom jeg har spørsmål eller ønsker å trekke tilbake samtykket mitt, vet jeg hvor jeg skal henvende meg."**

Kryss av her frivillig

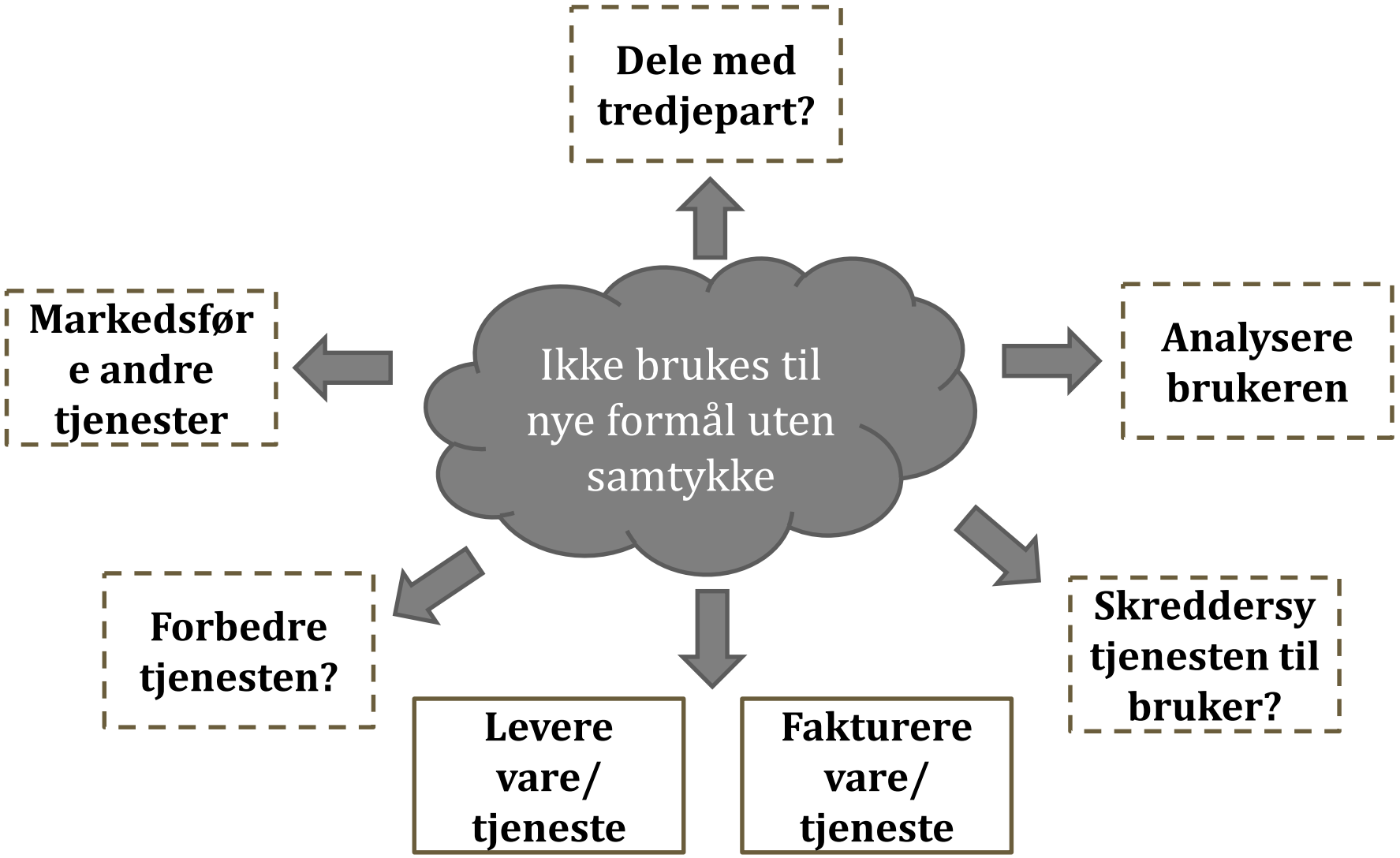
"Men vi får ikke plass til all informasjonen i et samtykke"

"Hvordan dokumenterer vi samtykket?"

"Er muntlig samtykke gyldig?"

"Ulike samtykke til ulike formål"?

Hva vil dere ha lov til å bruke dataene til?



Hvor lenge vil dere kunne lagre dataene?

"Ikke lengre enn det formålet tilsier"

Timer?

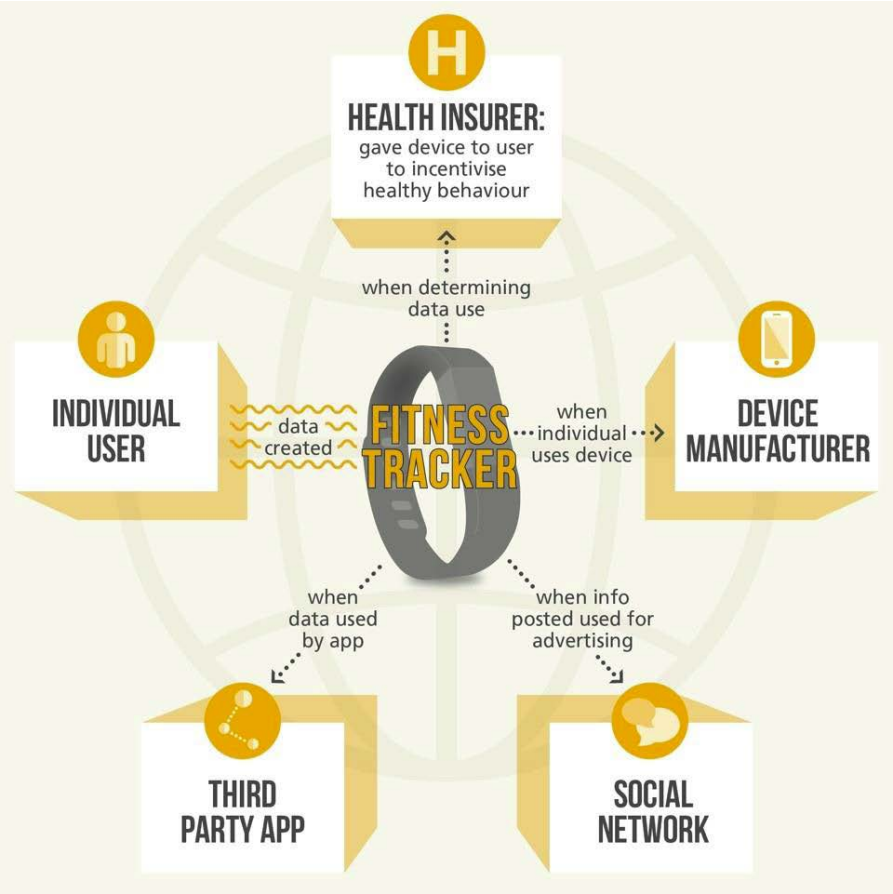
Dager?

Måneder?

År?

Evig tid?/Systemoppsett?

Hvem vil dere ha lov til å dele dataene med?



- ✓ Min virksomhet
- ✓ Mine underleverandører/ databehandlere
- ✓ Andre? Har du husket å spørre om lov?

  - ❑ App-utvikler?
  - ❑ Tjenesteleverandør?
  - ❑ Forsikringsselskap?
  - ❑ Reklamebyrå?
  - ❑ Dagligvarekjede?

Dagens opplegg

I. Hva er personvernforordningen?

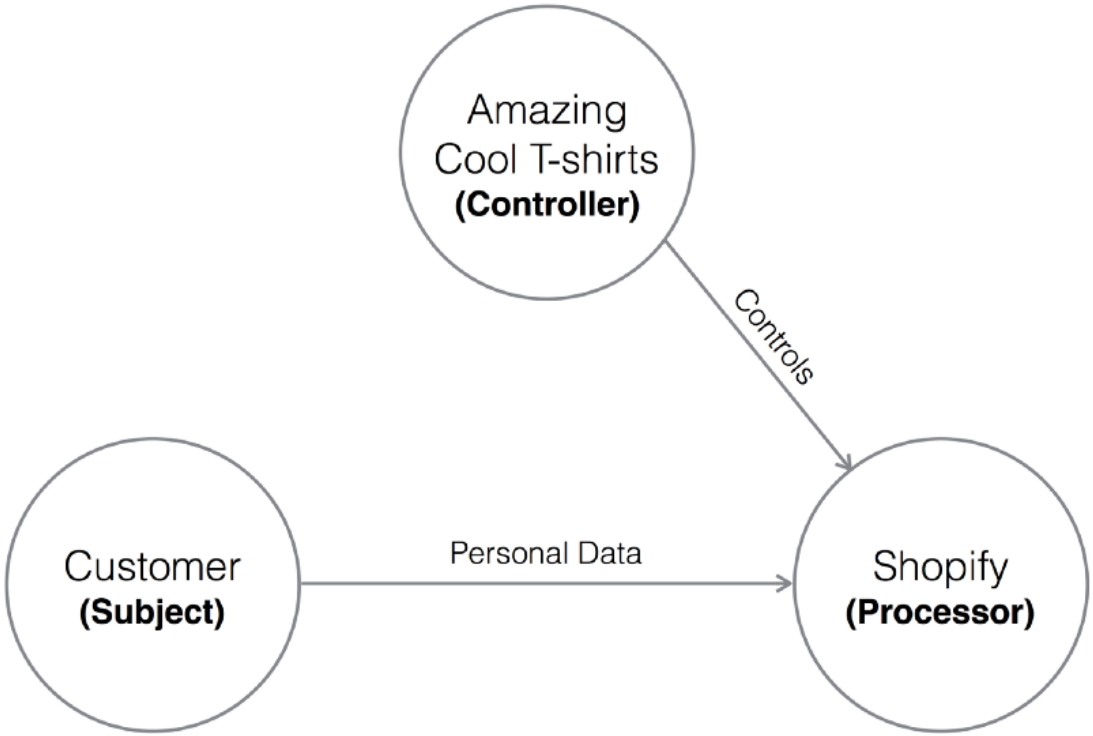
II. Hvordan går du frem for å oppfylle kravene i tide?

III. Hvilke grunnleggende krav stiller den til min virksomhet?

IV. Hva må jeg tenke på som a) "behandlingsansvarlig" og b) "databehandler"?

V. Hvilke rettigheter har "de registrerte"?

Hvilken rolle har din virksomhet ved behandling av personopplysninger?



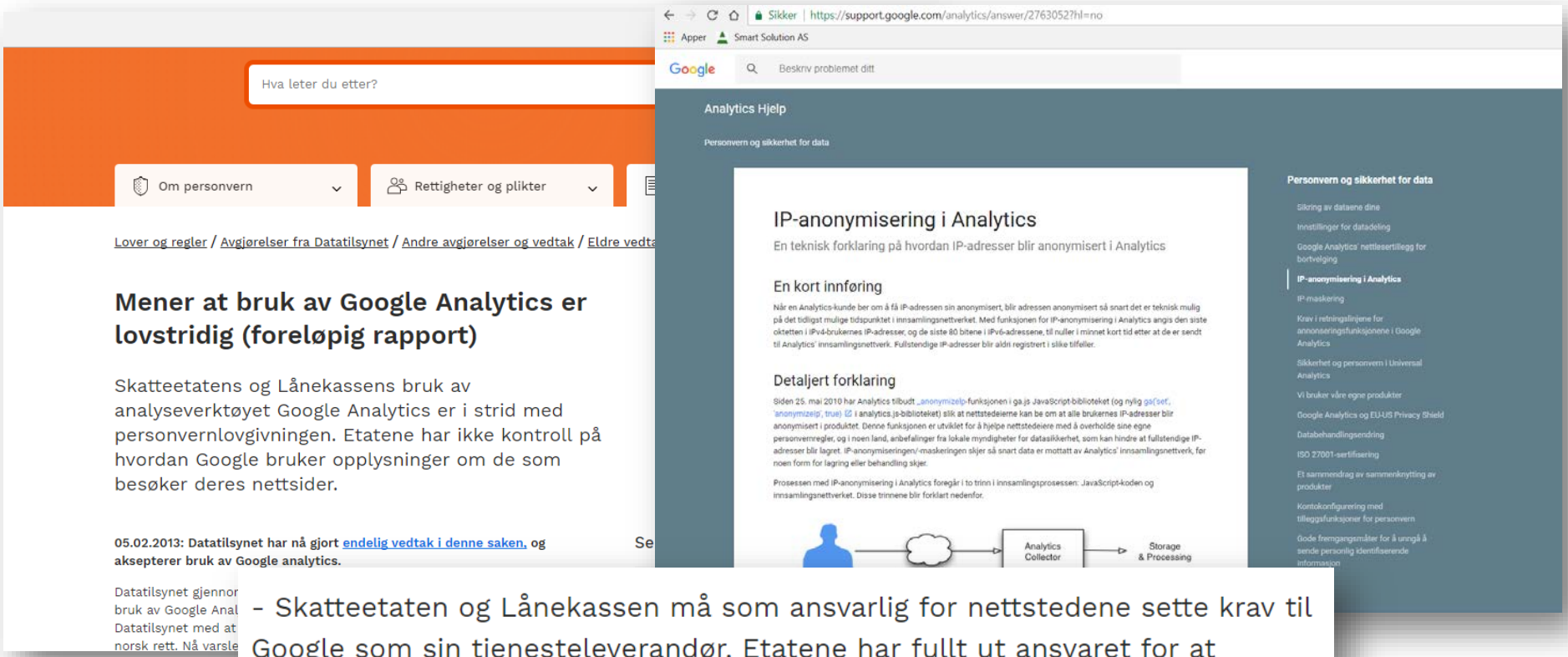
"Behandlings-ansvarlig"?

(Delt behandlingsansvar)

"Data-behandler"?

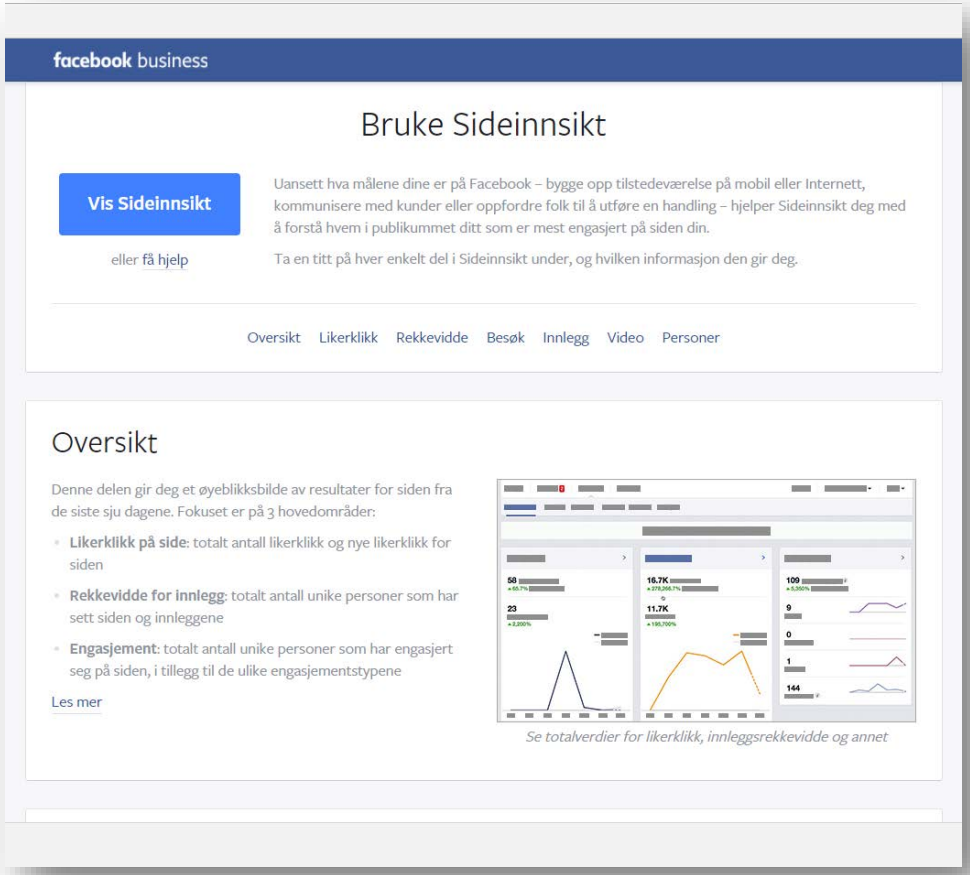
https://medium.com/wattx-stories/gdpr-what-your-company-should-know-and-do-starting-now-f62d70f72d7e

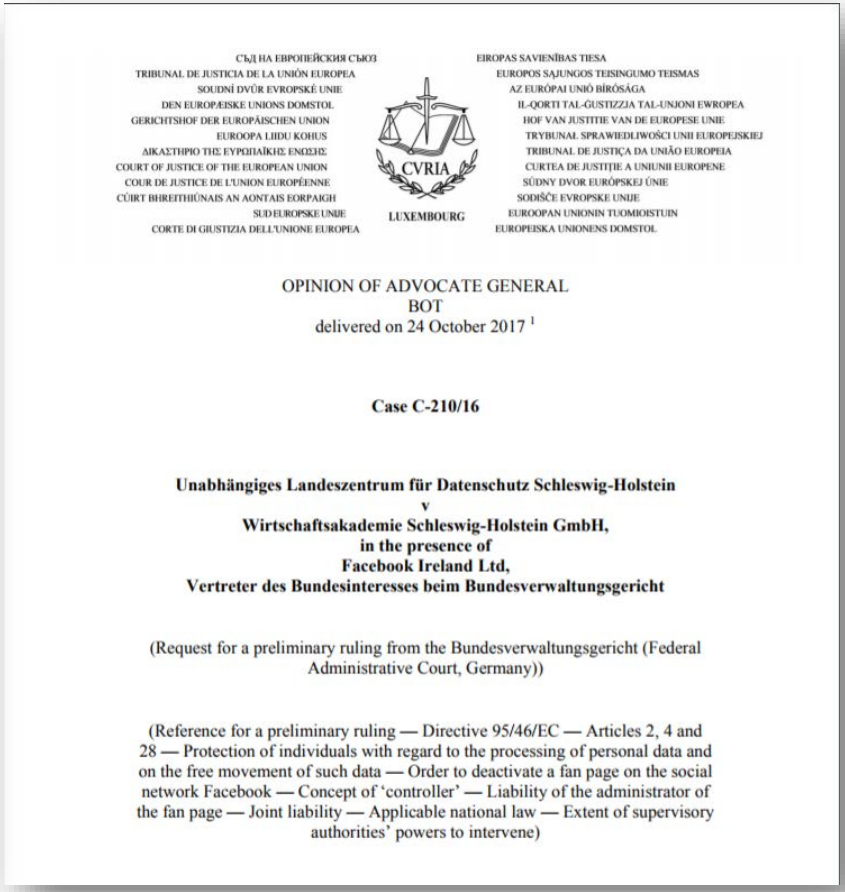
Hvilket ansvar har du for verktøyene du bruker? - Google Analytics



- Skatteetaten og Lånekassen må som ansvarlig for nettstedene sette krav til Google som sin tjenesteleverandør. Etatene har fullt ut ansvaret for at leverandøren behandler opplysningene i tråd med norsk lovgivning, sier Thon. Datatilsynet ber nå Lånekassen og Skatteetaten om å dokumentere at IP-adressene som samles inn anonymiseres og om å dokumentere at opplysningene ikke brukes til annet enn analyseformål.

Hvilket ansvar har du for verktøyene du bruker? Facebook fan pages/Insights




СЪД НА ЕВРОПЕЙСКИЯ СЪЮЗ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SOUDNÍ DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΔΙΚΑΣΤΗΡΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHREITHIÚNAIS AN AONTAIS EORPAIGH
SUD EUROPSKE UNIJE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA
EIROPAS SAVIENĪBAS TIESA
EUROPOS SĄJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-ĠUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAŁ SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EURÓPSKEJ ÚNIE
SODIŠČE EVROPSKE UNIJE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPEISKA UNIONENS DOMSTOL
CVRIA
LUXEMBOURG

OPINION OF ADVOCATE GENERAL
BOT
delivered on 24 October 2017 [1]

Case C-210/16

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
v
Wirtschaftsakademie Schleswig-Holstein GmbH,
in the presence of
Facebook Ireland Ltd,
Vertreter des Bundesinteresses beim Bundesverwaltungsgericht

(Request for a preliminary ruling from the Bundesverwaltungsgericht (Federal Administrative Court, Germany))

(Reference for a preliminary ruling — Directive 95/46/EC — Articles 2, 4 and 28 — Protection of individuals with regard to the processing of personal data and on the free movement of such data — Order to deactivate a fan page on the social network Facebook — Concept of 'controller' — Liability of the administrator of the fan page — Joint liability — Applicable national law — Extent of supervisory authorities' powers to intervene)

Hvilke krav stiller forordningen til deg som *"behandlingsansvarlig"*?

Informasjons-sikkerhet	Databehandler-avtale	Internkontroll	Varsling til DPA innen 72 timer
Regulere delt behandler-ansvar	Innebygget personvern	Personvern-rådgiver	Konsekvens-analyse

+ Dokumentasjon på at virksomheten følger reglene

Hvorfor er dokumentasjon så viktig for å oppfylle kravene?

"Det nye personvernregelverket legger vekt på **ansvarlighet og internkontroll** hos virksomheten fremfor forhåndskontroll fra Datatilsynet.« datatilsynet.no

KAN MISTE KONSESJONEN: Datatilsynet trekker tilbake Gjensidiges konsesjon dersom forsikringsselskapet ikke retter opp forholdene. (Foto: NTB Scanpix)

Gjensidige har fått kjempebot

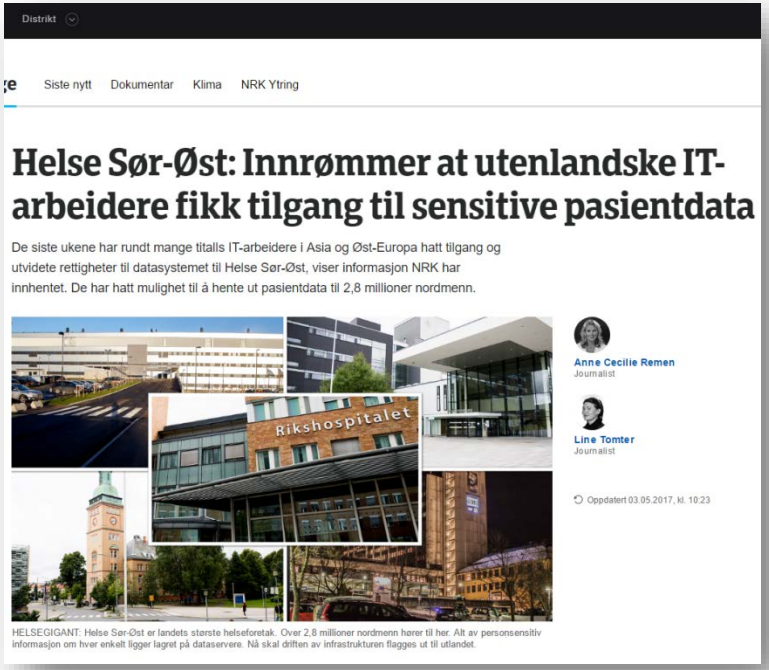
Datatilsynet gir rekordhøyt gebyr på 600.000 kroner til Gjensidige Forsikring, etter avdekking av ulovlige arbeidsmetoder.

Cathrine Eide 23.09.2013

Av Vilde Kalsaas Worren og Cathrine Eide

Datatilsynet mener forsikringsselskapet går for langt i sitt arbeid med å avdekke forsikringssvindel.

I tillegg mener de selskapet har for dårlig internkontroll.



"60 prosent svarer at de **ikke vet om de kan legge frem dokumentasjon** på hvordan deres bedrift håndterer personopplysninger eller at de vet at de ikke kan dokumentere hvordan de håndterer slike opplysninger." DN, 18.2.17

Hva skal virksomheten dokumentere?

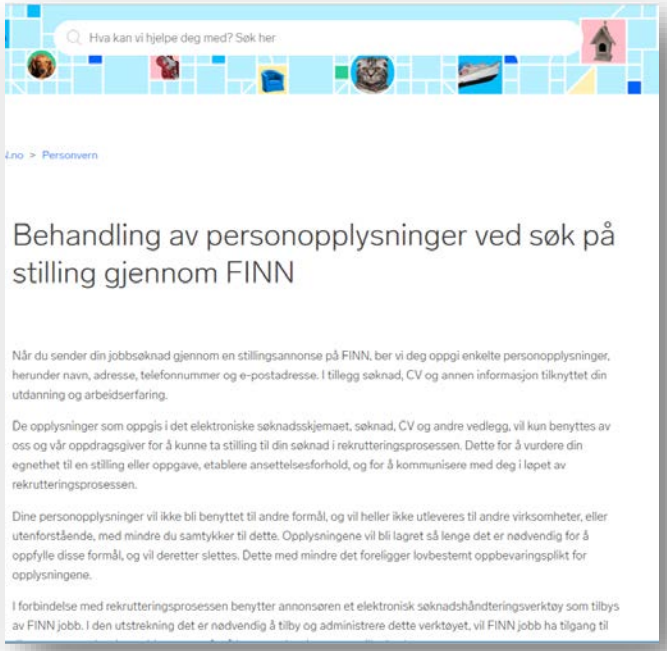
Internkontroll

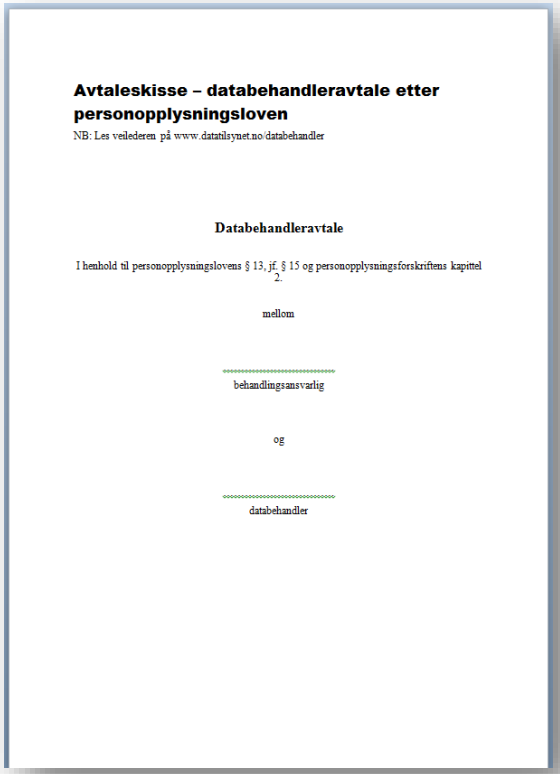
Dokumentasjon på dine tiltak for å sikre at du oppfyller lovens krav til behandling av personopplysninger

Informasjons-sikkerhet

Dokumentasjon på at du sikrer verdiene i de personopplysningene du behandler

Hva skal virksomheten dokumentere? (2)





Hvordan dokumenterer du internkontroll (personvern)?

ma/skjema-og-maler/maler-til-veileder-i-informasjonssikkerhet-og-internkontroll-i-word-/

Om personvern | Rettigheter og plikter | Regelverk og skje

Verktøy og skjema / Skjema og maler

Maler til veilederen i internkontroll og informasjonssikkerhet

Disse malene skal hjelpe virksomheter å få på plass *internkontroll* i egen virksomhet. Her kan du laste dem ned i word-, odt- eller pdf-format.

Publisert: 16.01.2012
Sist endret: 02.03.2016

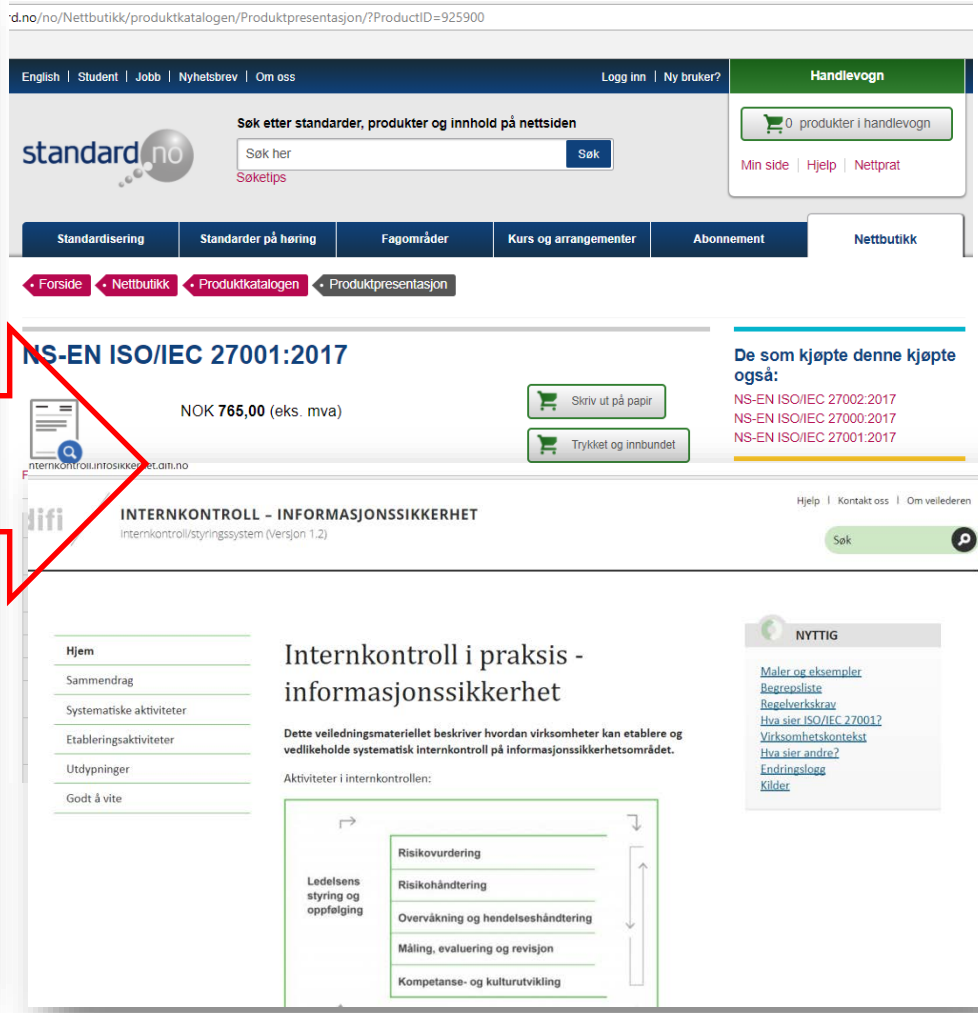
1. Word-maler

- Last ned alle word-malene til internkontroll og informasjonssikkerhet (zip)

Malene enkeltvis:

- Styringsdokument Internkontroll (1-01)
- Ledelsens gjennomgang (1-02)
- Sikkerhetsmål- og strategi (1-11)
- Sikkerhetsorganisasjon (1-12)
- Rutiner for håndtering av personopplysninger (2-01)
- Risikovurdering (2-11)

Hvordan dokumenterer du informasjonssikkerhet?



Hvilke krav stille GDPR til informasjonssikkerhet?

Virksomheten må etablere "egnede" fysiske og logiske tiltak

Virksomheten må håndtere risiko relatert til informasjonsverdier og personopplysninger

Sørge for **egnet sikkerhetsnivå ut fra risikoen** gjennom tekniske og organisatoriske tiltak, eks. ved pseudonymisering eller kryptering

Hvilke nye krav skal du oppfylle?

- **«Innebygget personvern»**

www. safedatamatters.com

- **Risikoanalyse**

https://brownglock.com/library/2016/06/15/gdpr-and-privacy-impact-assessments-why-are-they-required/

- **Varsle tilsyn innen 72 timer**

www.identitymanagementinstitute.org

- **Personvernrådgiver**

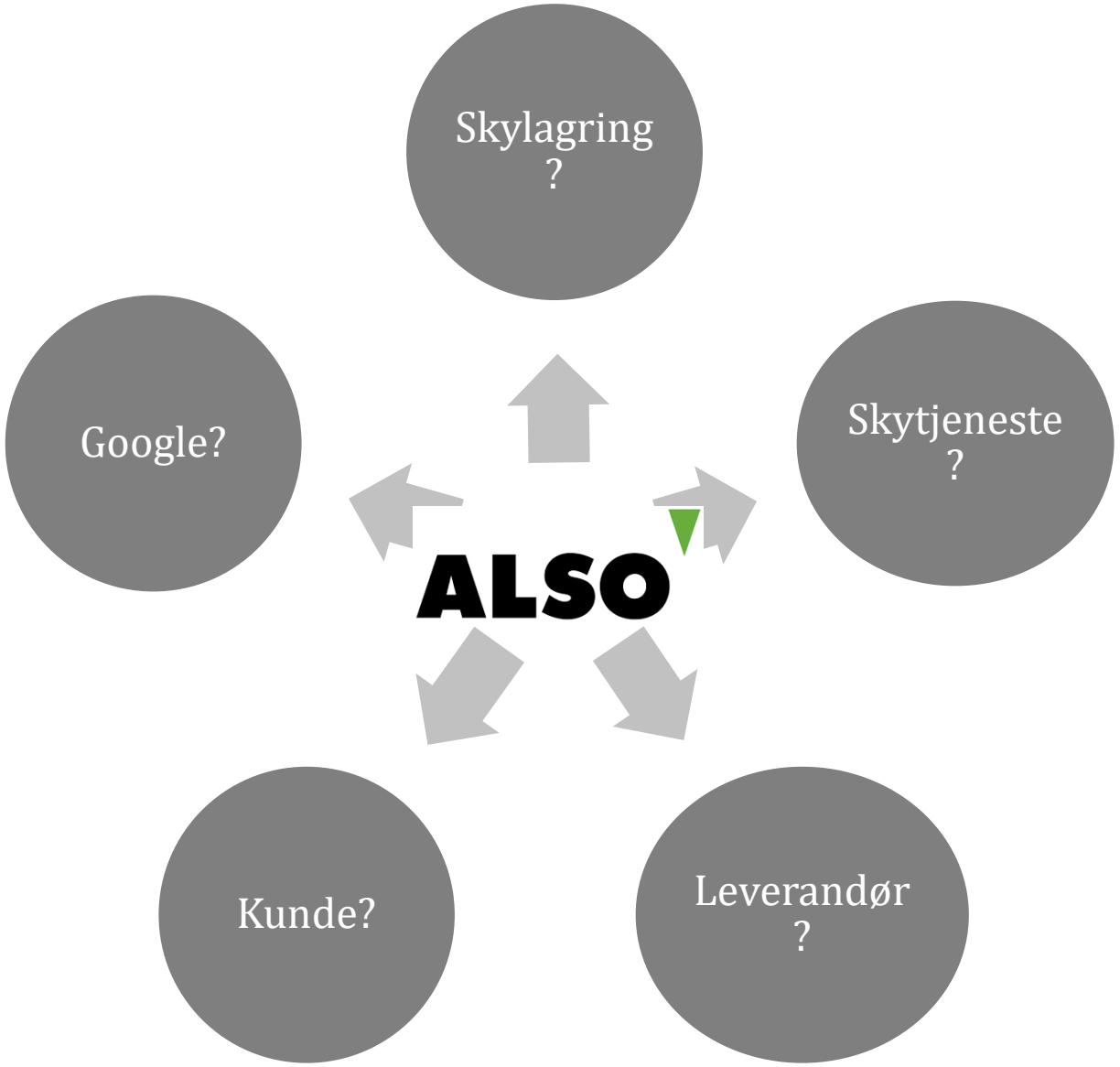
http://www.cpbuk.co.uk/

Hvilke krav stiller forordningen til deg som *"behandlingsansvarlig"*?

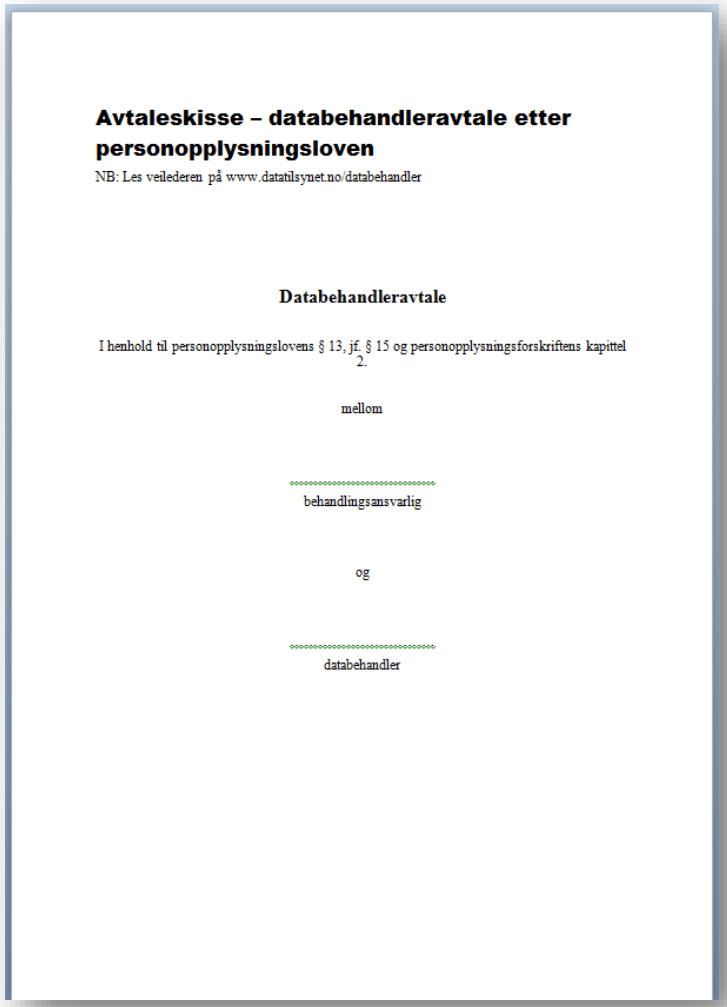
Informasjons-sikkerhet	Databehandler-avtale	Internkontroll	Varsling til DPA innen 72 timer
Regulere delt behandler-ansvar	Innebygget personvern	Personvern-rådgiver	Konsekvens-analyse

+ Dokumentasjon på at virksomheten følger reglene

Hvem må du inngå databehandleravtale med?



Hva skal databehandleravtalen min inneholde?



Avtaleskisse – databehandleravtale etter personopplysningsloven

NB: Les veilederen på www.datatilsynet.no/databehandler

Databehandleravtale

I henhold til personopplysningslovens § 13, jf. § 15 og personopplysningsforskriftens kapittel 2.

mellom

behandlingsansvarlig

og

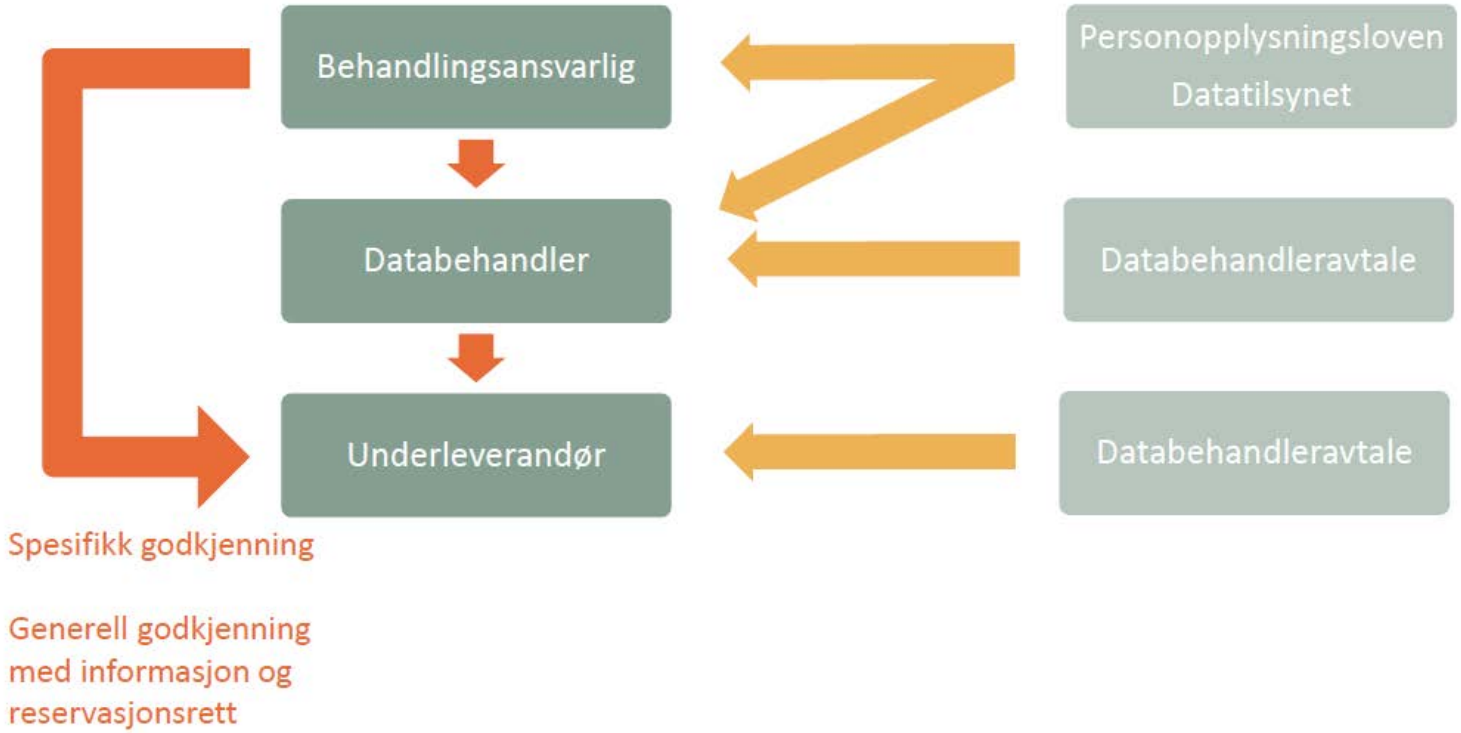
databehandler

Krav til databehandleravtalen

Forordningen stiller følgende krav til innholdet i en databehandleravtale:

- Databehandler skal kun behandler personopplysninger etter dokumenterte instruksjoner fra den behandlingsansvarlige.
- Databehandler skal kun overføre personopplysninger til et land utenfor EU-/EØS-området eller til internasjonale organisasjoner slik det er beskrevet i dokumenterte instruksjoner fra den behandlingsansvarlige.
- De som har tilgang til personopplysningene som behandles er underlagt taushetsplikt.
- Databehandler skal sørge for informasjonssikkerhet i tråd med artikkel 32.
- Databehandler må respektere reglene for underleverandører i tråd med artikkel 28.
- Avtalen skal spesifisere hvordan databehandler skal bistå den behandlingsansvarlige med å etterkomme krav fra enkeltpersoner.
- Avtalen skal spesifisere hvordan databehandler skal bistå den behandlingsansvarlige med informasjonssikkerhet, avvikshåndtering og konsekvensanalyse.
- Databehandler skal avhengig av hva den behandlingsansvarlige velger, slette eller tilbakeføre alle personopplysninger når databehandlingstjenestene opphører. Kopier skal også slettes. Dette gjelder med mindre en annen lov krever at de skal tas vare på.
- Databehandler skal tilgjengeliggjøre dokumentasjon som viser at de etterlever artikkel 28 for den behandlingsansvarlige. Databehandler skal også bidra til revisjoner.

Hva skal databehandleravtalen min inneholde? (3)



Dagens opplegg

I. Hva er personvernforordningen?

II. Hvordan går du frem for å oppfylle kravene i tide?

III. Hvilke grunnleggende krav stiller den til min virksomhet?

IV. Hva må jeg tenke på som a) "behandlingsansvarlig" og b) "databehandler"?

V. Hvilke rettigheter har "de registrerte"?

Hvilke krav stiller forordningen til deg som følge av *de registrertes rettigheter*?

Innsyn	Korrigering	Manuell behandling	Informasjon
Begrense behandlingen	Sletting/"bli glemt"	Protestere/ innsigelse	Data-portabilitet

Kostnadsfritt og innen én måned

Hvilke rettigheter er "nye" ?

- **Retten til å bli glemt**

http://www.cpbuk.co.uk/

- **Dataportabilitet**

https://www.greens-efa.eu/en/

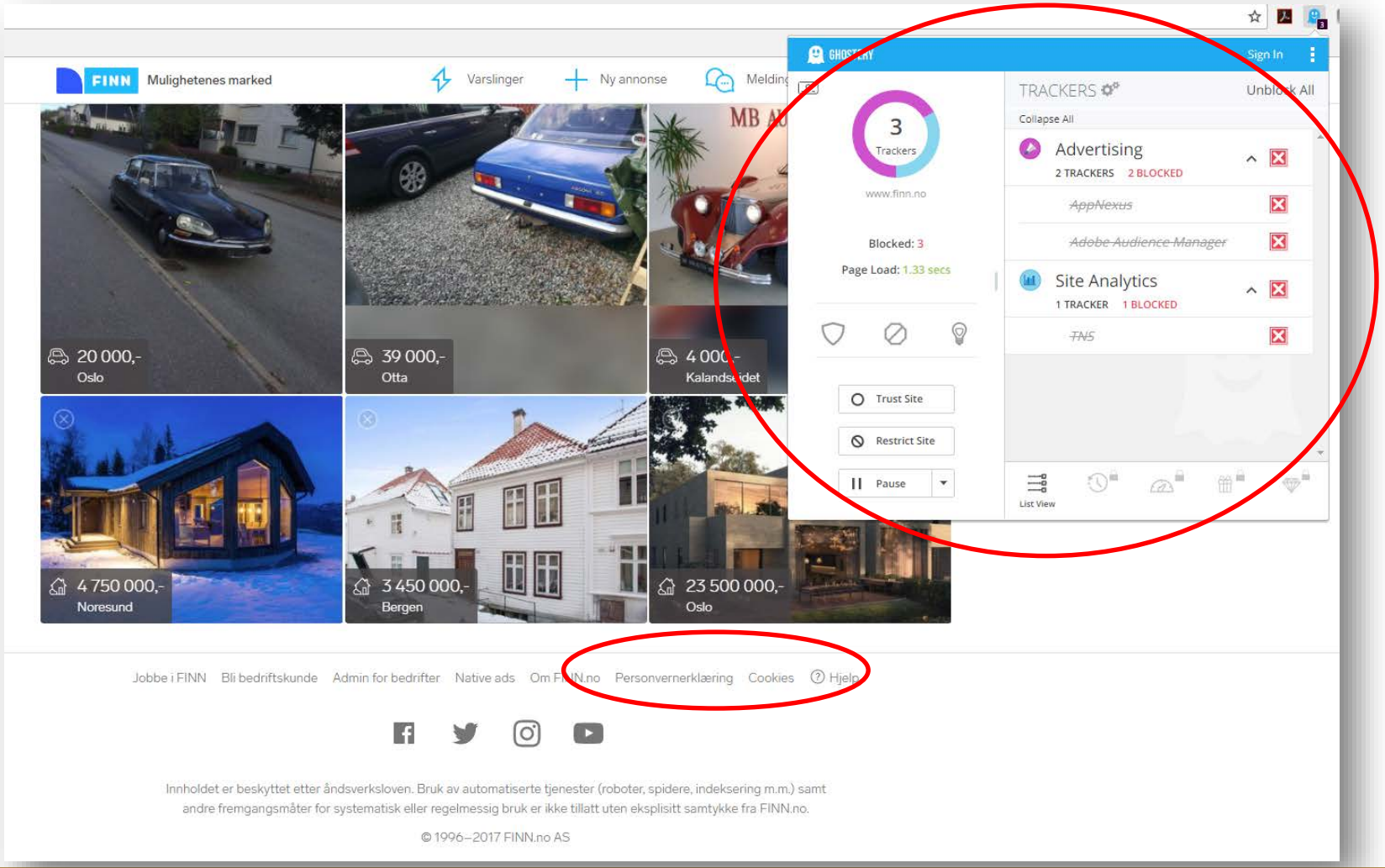
- **(Rett til å bli varslet)**

www.identitymanagementinstitute.org

- **(Unntak – begrunnet tvil om ID)**

http://easybankingtips.com/what-is-kyc-india/

Virksomheten må aktivt informere om behandlingen av personopplysninger



Ta kontakt hvis du har spørsmål

Jens Christian Gjesti
Tlf.: +47 902 02 072
Epost: jcg@kvale.no

View my LinkedIn® Profile

Kvale Advokatfirma DA
Haakon VIIs gate 10
0161 Oslo
Tlf. +47 22 47 97 00

www.kvale.no/kompetanse/fagomrader/personvern/

www.personverntesten.no