



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?

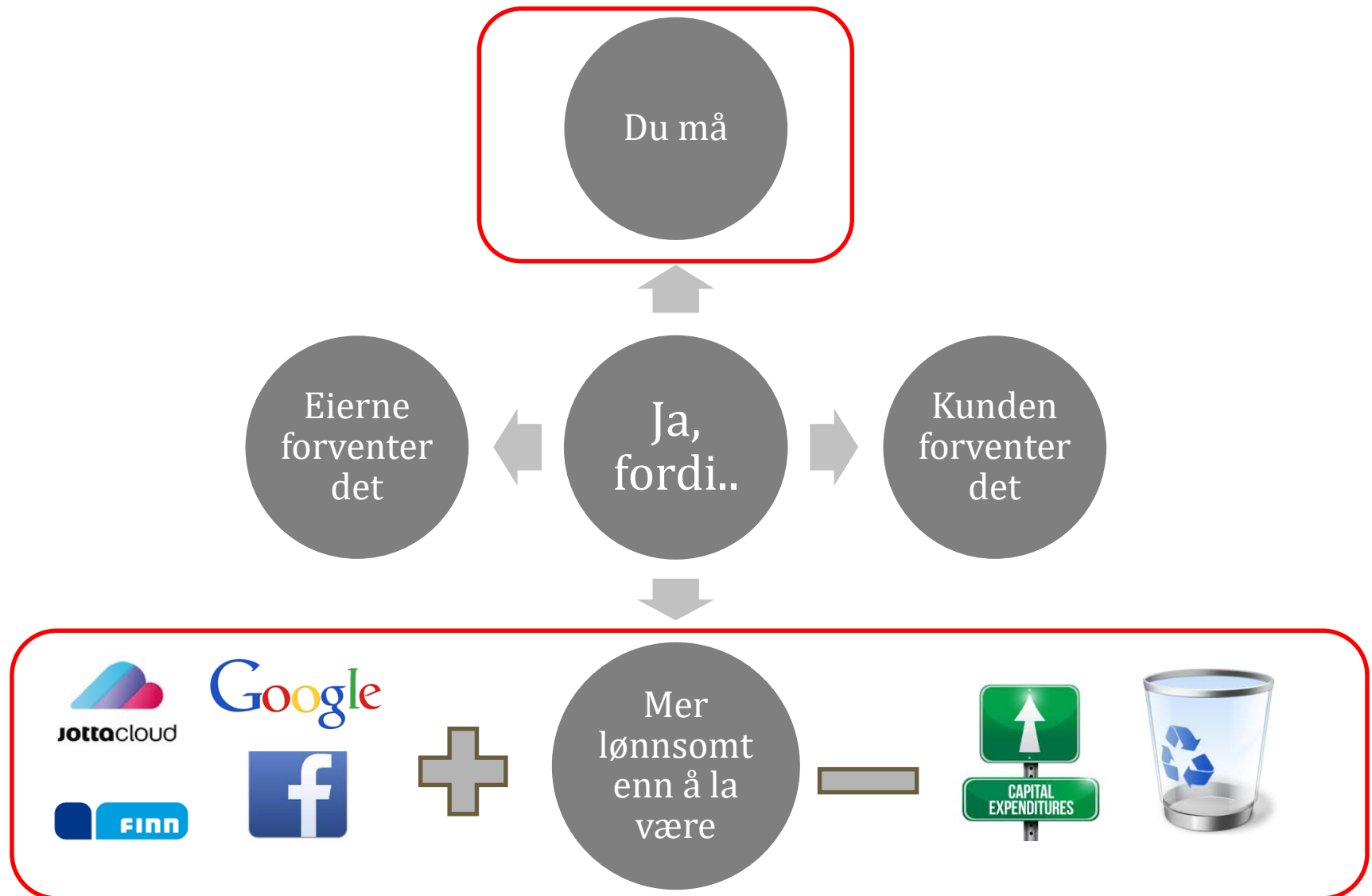
- EU-forordning som norsk lov
- ..supplert med nasjonale tilpasninger (CCTV mv.)

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)

IT-sikkerhetsjef i Atea, Thomas Tømmernes

De som ikke har fått med seg dette risikerer bøter på inntil 20 millioner

GDPR – EUs personvernforordning:

Personvernet er viktig for oss alle, og for ansatte i bedriften. Når Datatilsynet kommer på visitt må virksomheten ha prosedyrene og rutinene i orden. (Bilde: Colourbox)

Nye EU-regler gir fare for gigantbøter

Kampanje

Tech / Publisert 20.02.2017 21:29:51 - Oppdatert 21.02.2017 07:09:27

- Tar du bota?

- Nye personvernregler vil få store konsekvenser for virksomheter som lagrer kundedata, skriver Nils Ola Bark.

KOMMENTAR



Nils Ola Bark
Markedsdirektør, Atea

25. mai 2018 trer nye personvernregler i form av EU-forordningen GDPR i kraft. Dette får store konsekvenser for norske virksomheter som lagrer data om sine kunder, trolig de aller fleste norske selskaper av en viss størrelse.

Sankjonsregimet er hissig. Datatilsynet vil kunne ilegge bøter på opp til fire prosent av selskapets omsetning. For oss i Atea vil det være et beløp på i overkant av 300 millioner. En anselig sum, katastrofe for vårt resultat og totalt ødeleggende for vårt omdømme. Jeg tipper vårt styre og våre aksjonærer ville sett svært alvorlig på det også. Så hos oss skal ikke dette skje!

til neste år.

iktig kompetanse
ette innslått i hva EUs nye
PR handler om, viser en
redtiledere i privat og
Analyse har gjort for

edriftsledere sier de har
enforordningen.

de ikke vet om de kan
tasjen på hvordan
personopplysninger eller at
dokumentere hvordan de
sninger.

Virksomheter har startet
å se seg den nye, svært
egen GDPR, til tross for at

etere. Det

Kommentarer (0)

nice
ittsteknologi

dataene dine til å
inere deg
aken

— 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?

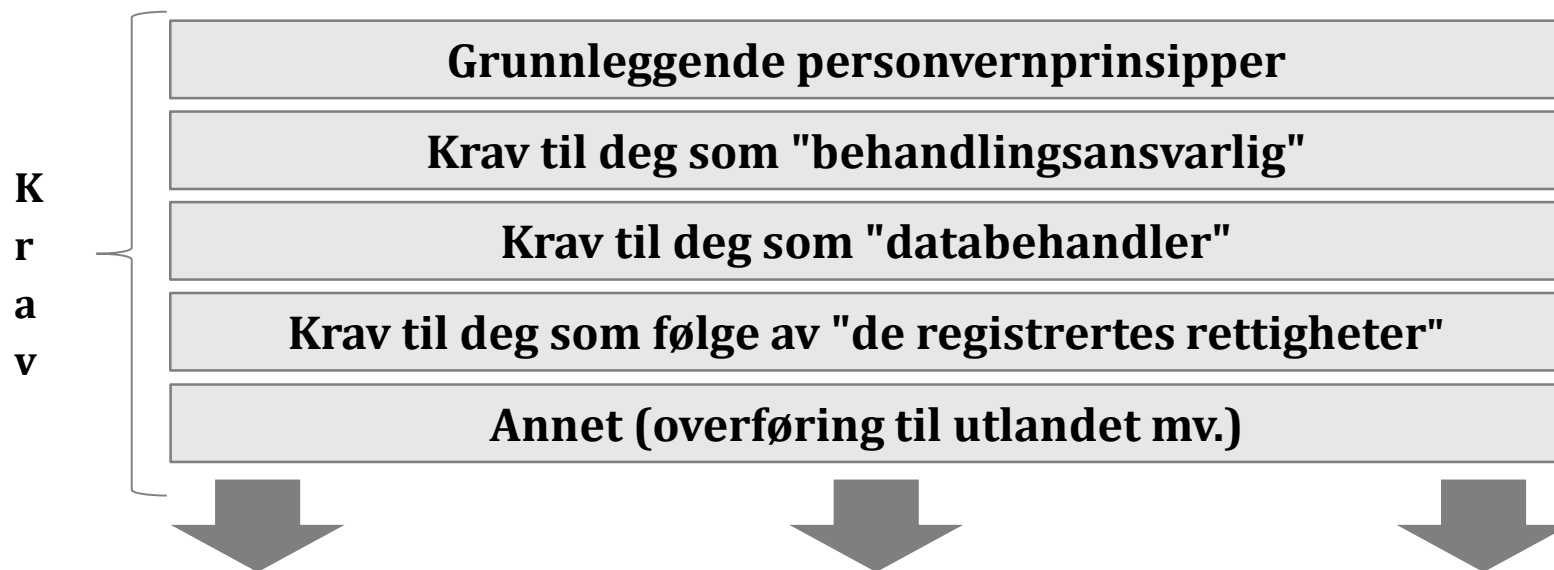
II. Hvordan går du frem for å oppfylle kravene i tide?

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?



L
e
v
e
r
a
n
s
e

A) Dokumentasjon

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

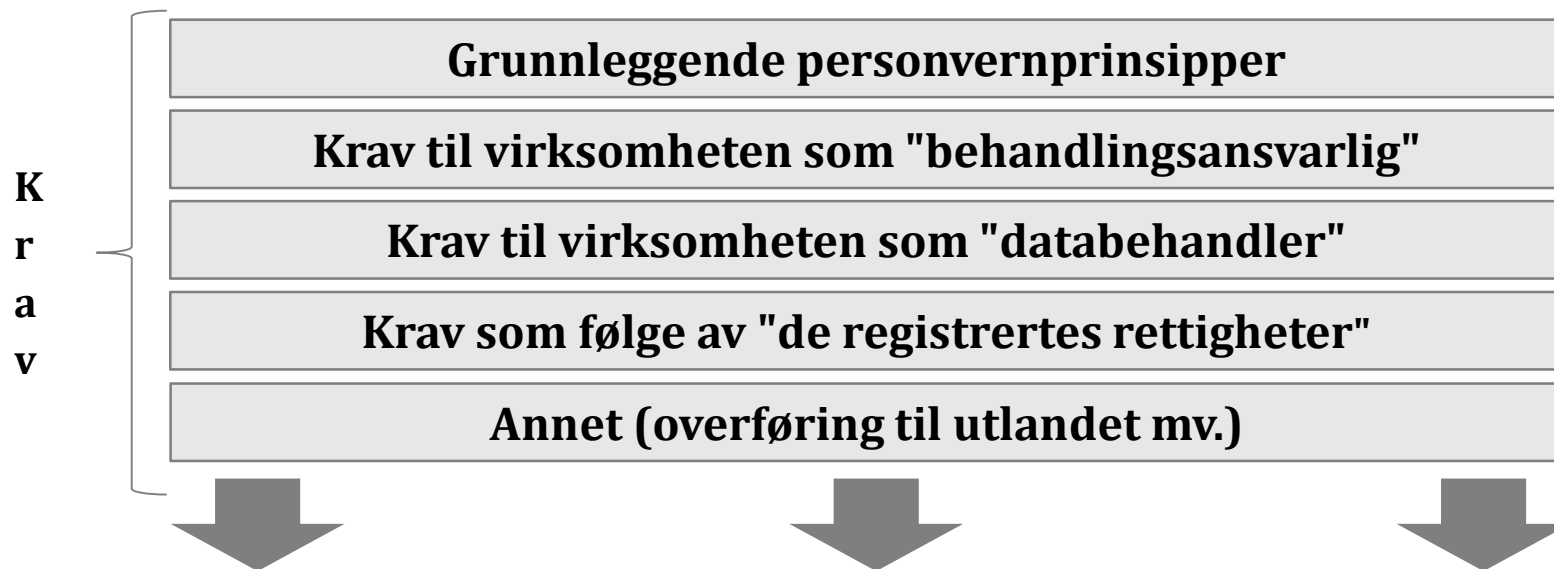
B) Organisatoriske tiltak

- 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?



L
e
v
e
r
a
n
s
e

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 rutineene når reglene trer i kraft.

2
Alle skal ha en forståelig personvern-erklæring
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 barns 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 oppdragsgjveren sin hvis de får instruksjoner som er i strid med loven. Oppdragsgjver skal også godkjenne databehandlerens underleverandører. Databehandlere kan også bli holdt økonomisk ansvarlig sammen med oppdragsgjver.

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 rutineene på plass. Datatilsynet skal godkjenne bransjenormene.

9
Alle får nye krav til avvikhåndtering
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 oppfører 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. Sørge for å ha en slik oversikt. Det er et krav som gjelder også etter dagens lov.

2
Sørge 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 artikkel om de nye reglene etter hvert som vi utarbeider dem.

4
Lag rutiner for å følge de nye reglene
Gå gjennom rutineene dere har for behandling av personopplysninger. Oppdater dem etter nytt regelverk der det trengs. Dokumenter de nye rutineene, 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 borgere 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

Hvordan får dere oversikt over hvordan dere ligger an?

www.personverntesten.no

personverntesten.no

Apper Smart Solution AS

KVALE Personverntesten Bestill et gratis møte

108 dager igjen




- til de nye personvernreglene trer i kraft

Hvor godt forberedt er din virksomhet på den nye personvernforordningen (GDPR)?

- ✓ Få et overblikk med utgangspunkt i din virksomhets egen situasjon
- ✓ Få våre innspill til hva dere bør gjøre fremover

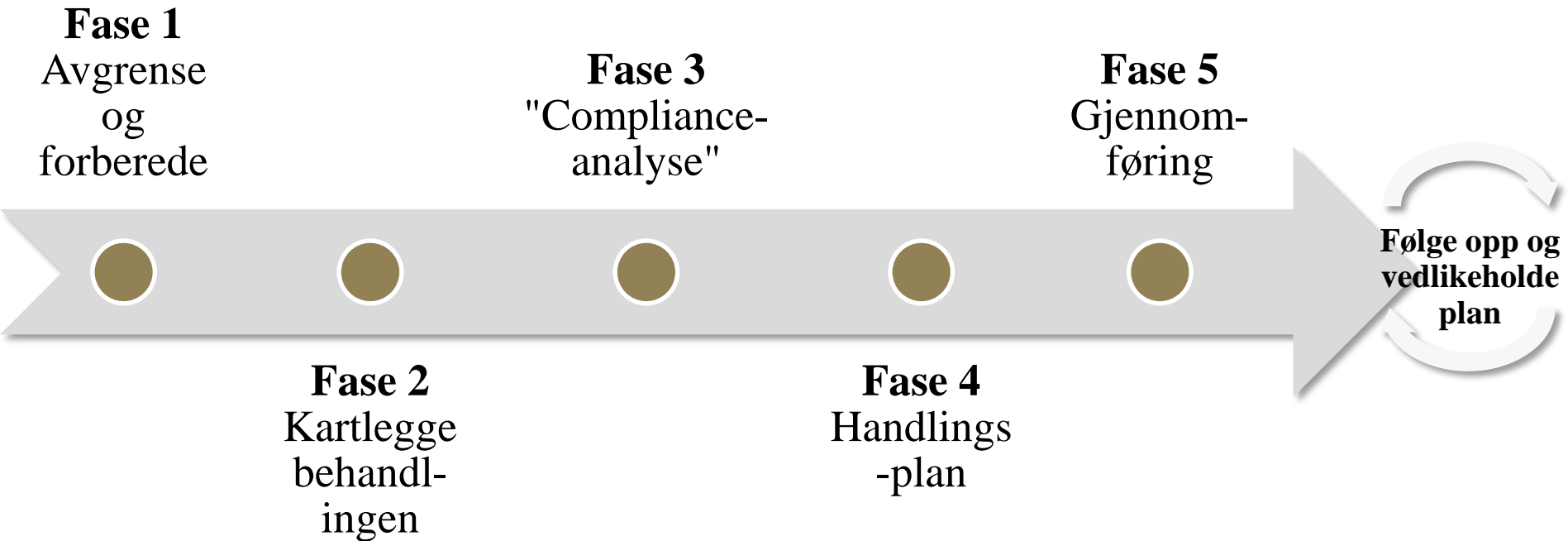
Start testen

Slik kan vi hjelpe deg

 <p>Oppfyller din virksomhet kravene i den nye personvernforordningen?</p> <p>Ta testen</p>	 <p>Bestill et gratis møte med våre eksparter</p> <p>Bestill møte</p>	 <p>Bli godt forberedt på den nye personvernforordningen</p> <p>Se våre kurs</p>
--	--	---

Nyheter

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/ Konesjon	Sensitive person-opplysninger	Sikkerhets-tiltak	Lagring og kommunikasjon	Opplysningenes omfang	Avdeling	System-/ dataeier
Lønn og personal: - lønnsopplysninger - personal-opplysninger	Personopplysningsloven, § 8f	Unntatt i forskriftens § 7-16	Nei			Ca. 130 ansatte		
Barnevern: - vurdering og tiltak	Barnevernloven, § 3-1	Meldt 14.01.2009	Ja			Ca. 68 barn og foresatte		
Helseopplysninger: - pasient-journal	Helsepersonelloven § 39 flg.	Meldt 14.01.2009	Ja			Ca. 413 pasienter		
Elevedministrasjon - elever / foresatte - lærere	Opplæringsloven § 13-5		Ja			Ca. 219 søkere		
Hendelsesregister: - logg over brudd	Personopplysningsloven, § 13	Unntatt i forskriftens § 7-11	Nei			Arkivlogg, nettverkslogg og serverlogg, PC-logger		
Kundeopplysninger - Salgskonkatter - Leveranse-kontakter	Personopplysningsloven, § 8 a		Nei			Ca. 8000		

MER SPESIFIKT SKAL OVSERIKTEN GI KORTFATTET INFORMASJON OM

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

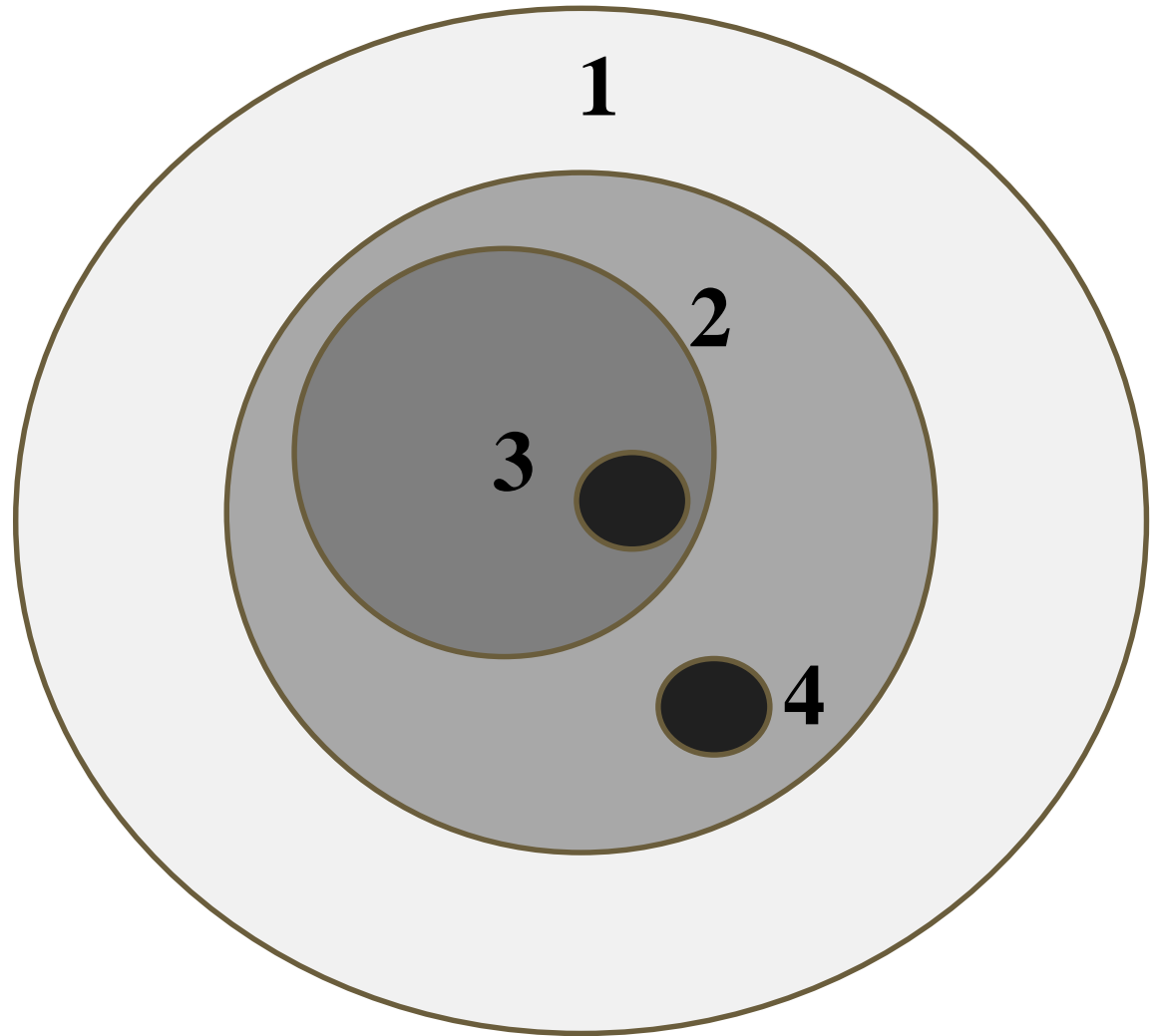
EKSEMPEL PÅ FREMGANGSMÅTE FOR KARTLEGGING AV BEHANDLINGER:

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

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 behandler 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"

Vil dine data være personopplysninger?

Kundebase	<ul style="list-style-type: none">• Navn, adresse, kjønn, fødselsnummer, fakturadato, abonnement, dialog med kundeservice, opptak mv.	✓
Informasjon om transaksjoner	<ul style="list-style-type: none">• Vare/tjeneste, dato, sum, antall kjøp, betalingsmåte, reklamasjoner mv.	✓
Metadata	<ul style="list-style-type: none">• IP-adresse, MAC-adresse, telefonnr., tidspunkt, lengde, type tjeneste, lokasjon, CDR, mv.	✓
Analyse/"profilering" av kunden	<ul style="list-style-type: none">• 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

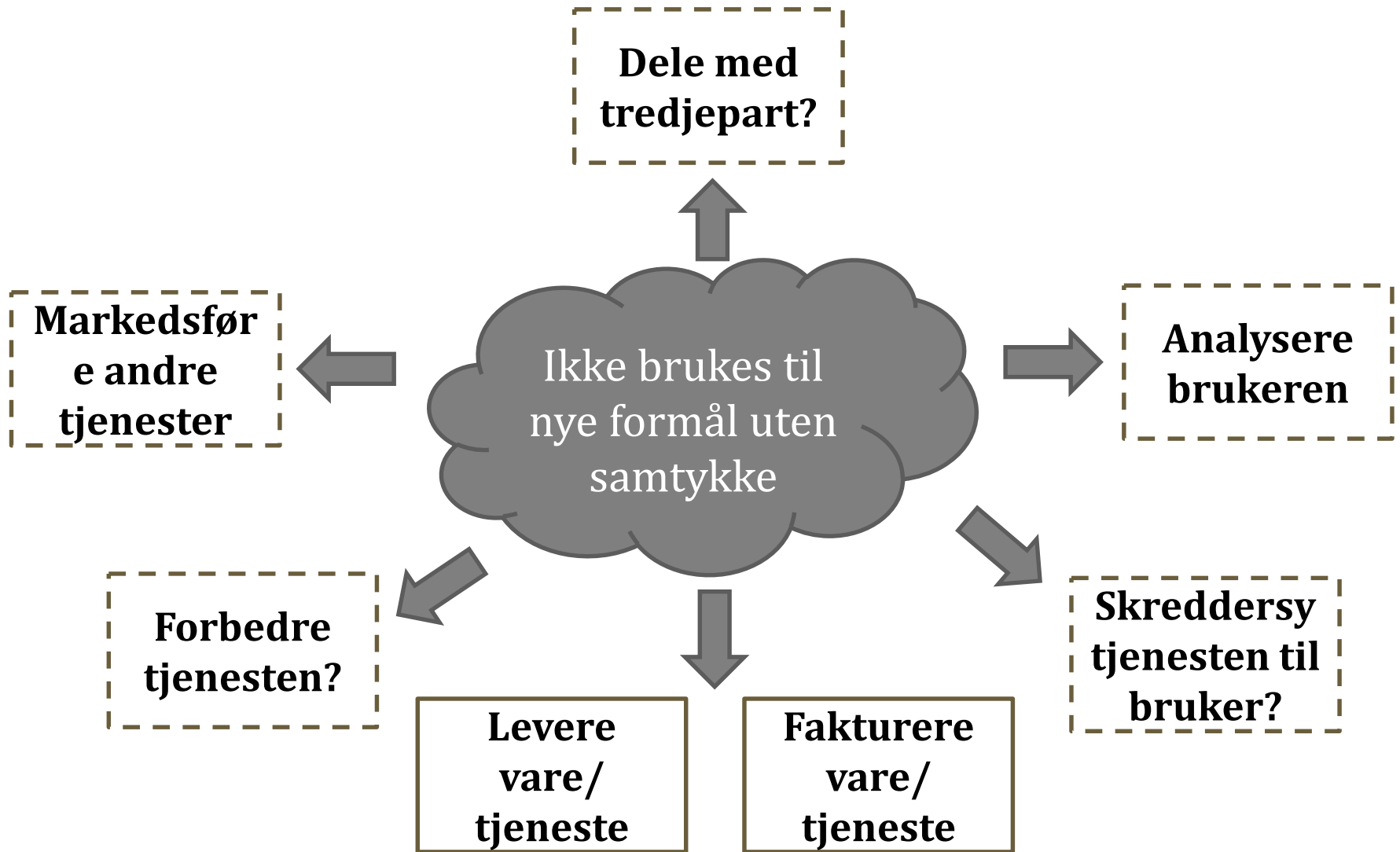
"Men vi får ikke plass til all informasjonen i et samtykke"

"Hvordan dokumenterer vi samtykket?"

"Er muntlig samtykke gyldig?"

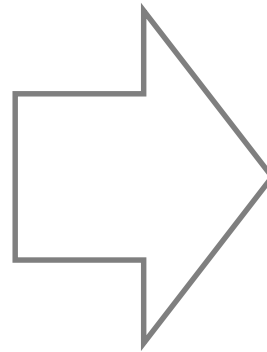
"Ulike samtykke til ulike formål"?

Hva vil dere ha lov til å bruke dataene til?



Hvor lenge vil dere kunne lagre dataene?

"Ikke lengre enn det formålet tilsier"



Timer?

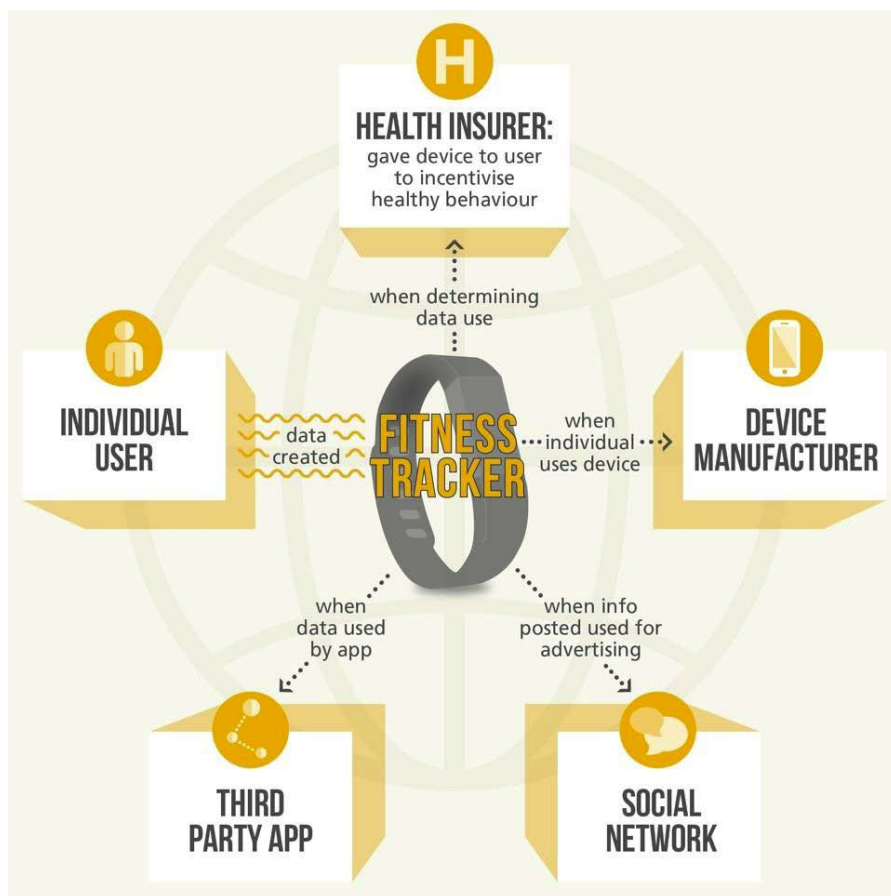
Dager?

Måneder?

År?

Evig tid?/Systemoppsett?

Hvem vil dere ha lov til å dele dataene med?



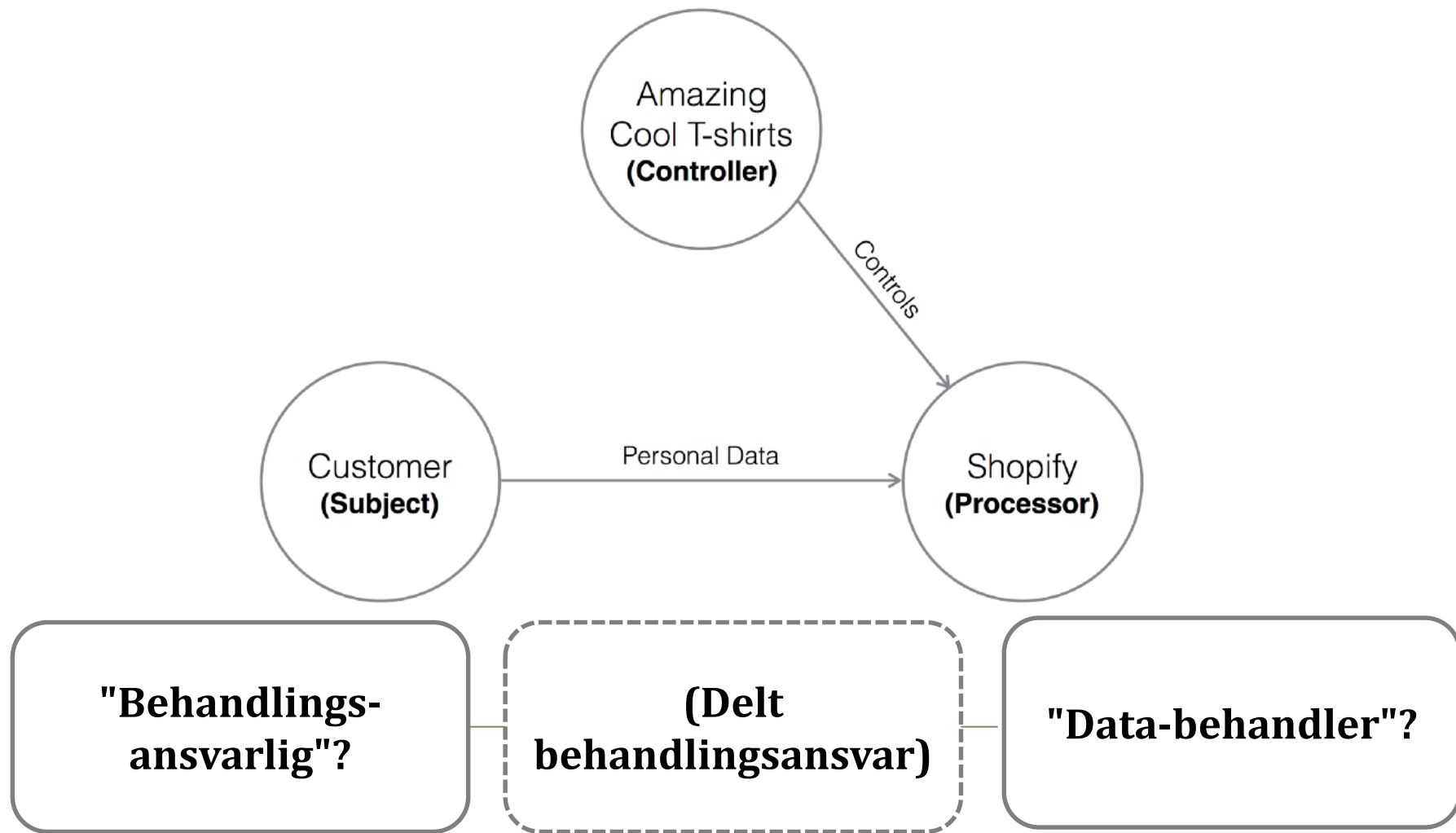
- ✓ Min virksomhet
- ✓ Mine underleverandører/
databehandlere
- ✓ Andre? Har du husket å spørre om lov?

- App-utvikler?
- Tjenesteleverandør?
- Forsikringselskap?
- 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?



<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

The image shows two overlapping web pages. On the left is a page from the Norwegian Data Protection Authority (Datatilsynet) with an orange header and a search bar. The main heading reads 'Mener at bruk av Google Analytics er lovstridig (foreløpig rapport)'. Below it, there is a paragraph about the tax authority and loan office's use of Google Analytics being in conflict with the personal data protection law. A date '05.02.2013' is also visible. On the right is a screenshot of the Google Analytics help page titled 'IP-anonymisering i Analytics'. It explains that IP addresses are anonymized in Analytics and provides a technical overview and a detailed explanation of the process. A diagram at the bottom of the help page shows the flow from a user to the Analytics Collector and then to Storage & Processing.

- 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

facebook business

Bruke Sideinnsikt

[Vis Sideinnsikt](#)

Uansett hva målene dine er på Facebook – bygge opp tilstedeværelse på mobil eller Internett, kommunisere med kunder eller oppfordre folk til å utføre en handling – hjelper Sideinnsikt deg med å forstå hvem i publikkummet ditt som er mest engasjert på siden din.

eller [få hjelp](#)

Ta en titt på hver enkelt del i Sideinnsikt under, og hvilken informasjon den gir deg.


Oversikt Likerklikk Rekkevidde Besøk Innlegg Video Personer

Oversikt

Denne delen gir deg et øyeblikksbilde av resultater for siden fra de siste sju dagene. Fokuset er på 3 hovedområder:


- Likerklikk på side: totalt antall likerklikk og nye likerklikk for siden
- Rekkevidde for innlegg: totalt antall unike personer som har sett siden og innleggene
- Engasjement: totalt antall unike personer som har engasjert seg på siden, i tillegg til de ulike engasjementstypene

[Les mer](#)



Se totalverdier for likerklikk, innleggsrekkevidde og annet

ЦІЛІ НА ЕВРОПЕЙСЬКІЙ СІМОРІ
TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA
SÚDNI DVŮR EVROPSKÉ UNIE
DEN EUROPÆISKE UNIONS DOMSTOL
GERICHTSHOF DER EUROPÄISCHEN UNION
EUROOPA LIIDU KOHUS
ΑΡΧΑΪΘΠΙΟ ΤΗΣ ΕΥΡΩΠΑΪΚΗΣ ΕΝΩΣΗΣ
COURT OF JUSTICE OF THE EUROPEAN UNION
COUR DE JUSTICE DE L'UNION EUROPÉENNE
CÚIRT BHRÉITHÉONAIS AN AONTAIS EORPAIGH
SUD-EUROPSKE UNIE
CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA



LUXEMBOURG

EROPAS SAVIENĪBAS TIESA
EUROPOS SAJUNGOS TEISINGUMO TEISMAS
AZ EURÓPAI UNIÓ BÍRÓSÁGA
IL-QORTI TAL-GUSTIZZJA TAL-UNJONI EWROPEA
HOF VAN JUSTITIE VAN DE EUROPESE UNIE
TRYBUNAL SPRAWIEDLIWOŚCI UNII EUROPEJSKIEJ
TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA
CURTEA DE JUSTIȚIE A UNIUNII EUROPENE
SÚDNY DVOR EVROPSKEJ UNIE
SODISČE EVROPSKE UNIE
EUROOPAN UNIONIN TUOMIOISTUIN
EUROPESKA UNIONENS DOMSTOL

OPINION OF ADVOCATE GENERAL BOT delivered on 24 October 2017¹

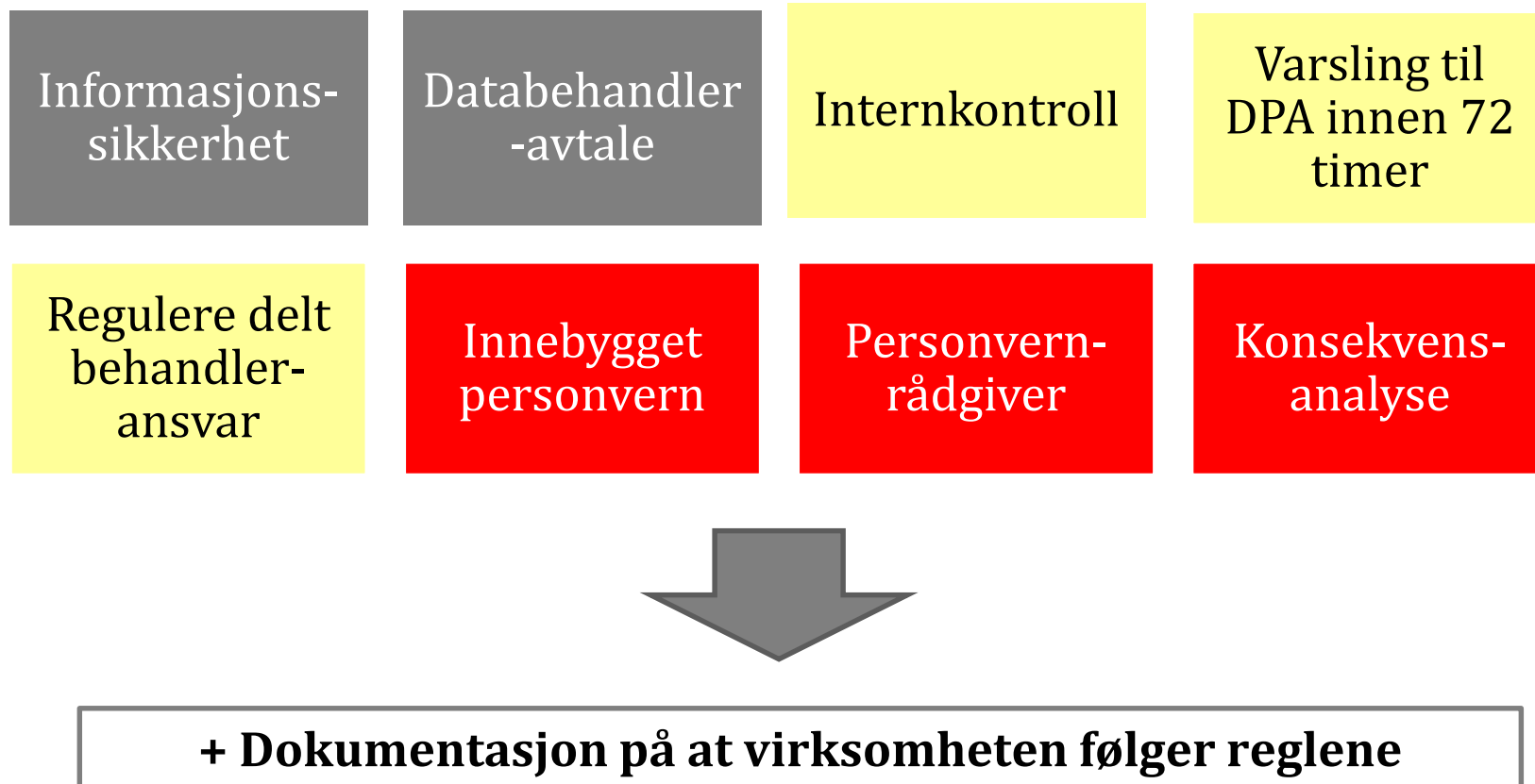
Case C-210/16

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))

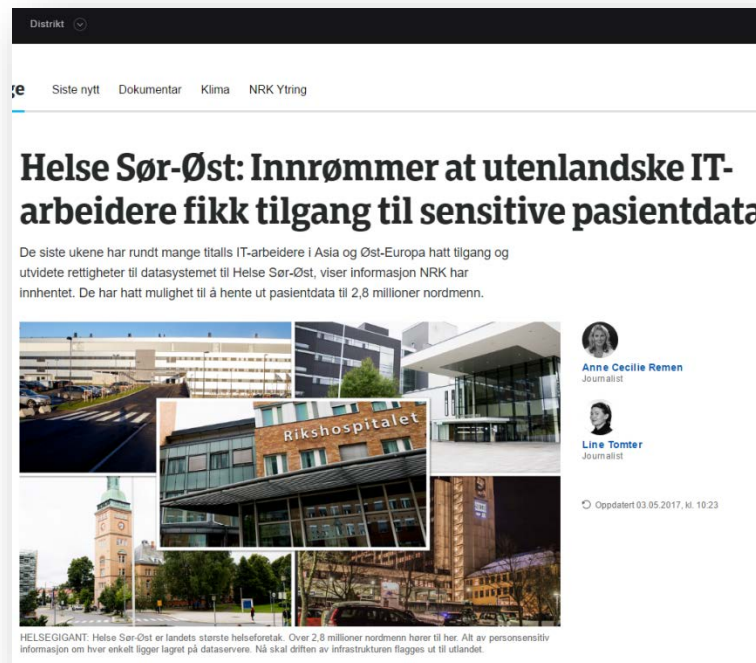
(Reference for a preliminary ruling — Directive 95/46/EC — Articles 2, 4 and 28 — Protection of individuals with regard to the processing of personal data and on the free movement of such data — Order to deactivate a fan page on the social network Facebook — Concept of ‘controller’ — Liability of the 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"*?



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



"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?



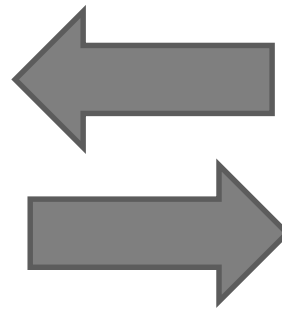
Internkontroll

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)



Hva kan vi hjelpe deg med? Søk her

Leno > Personvern

Behandling av personopplysninger ved søk på stilling gjennom FINN

Når du sender din jobbsøknad gjennom en stillingsannonse på FINN, ber vi deg oppgi enkelte personopplysninger, herunder navn, adresse, telefonnummer og e-postadresse. I tillegg søknad, CV og annen informasjon tilknyttet din utdanning og arbeidserfaring.

De opplysninger som oppgis i det elektroniske søknadsskjemaet, søknad, CV og andre vedlegg, vil kun benyttes av oss og vår oppdragsgiver for å kunne ta stilling til din søknad i rekrutteringsprosessen. Dette for å vurdere din egnethet til en stilling eller oppgave, etablere ansettelsesforhold, og for å kommunisere med deg i løpet av rekrutteringsprosessen.

Dine personopplysninger vil ikke bli benyttet til andre formål, og vil heller ikke utleveres til andre virksomheter, eller utenforstående, med mindre du samtykker til dette. Opplysningene vil bli lagret så lenge det er nødvendig for å oppfylle disse formål, og vil deretter slettes. Dette med mindre det foreligger lovbestemt oppbevaringsplikt for opplysningene.

I forbindelse med rekrutteringsprosessen benytter annonsøren et elektronisk søknadshåndteringsverktøy som tilbys av FINN jobb. I den utstrekning det er nødvendig å tilby og administrere dette verktøyet, vil FINN jobb ha tilgang til



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



Consent
I agree

Hvordan dokumenterer du internkontroll (personvern)?



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

Om personvern | Rettigheter og plikter | Regelverk og skjema

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 \(zip\)](#)

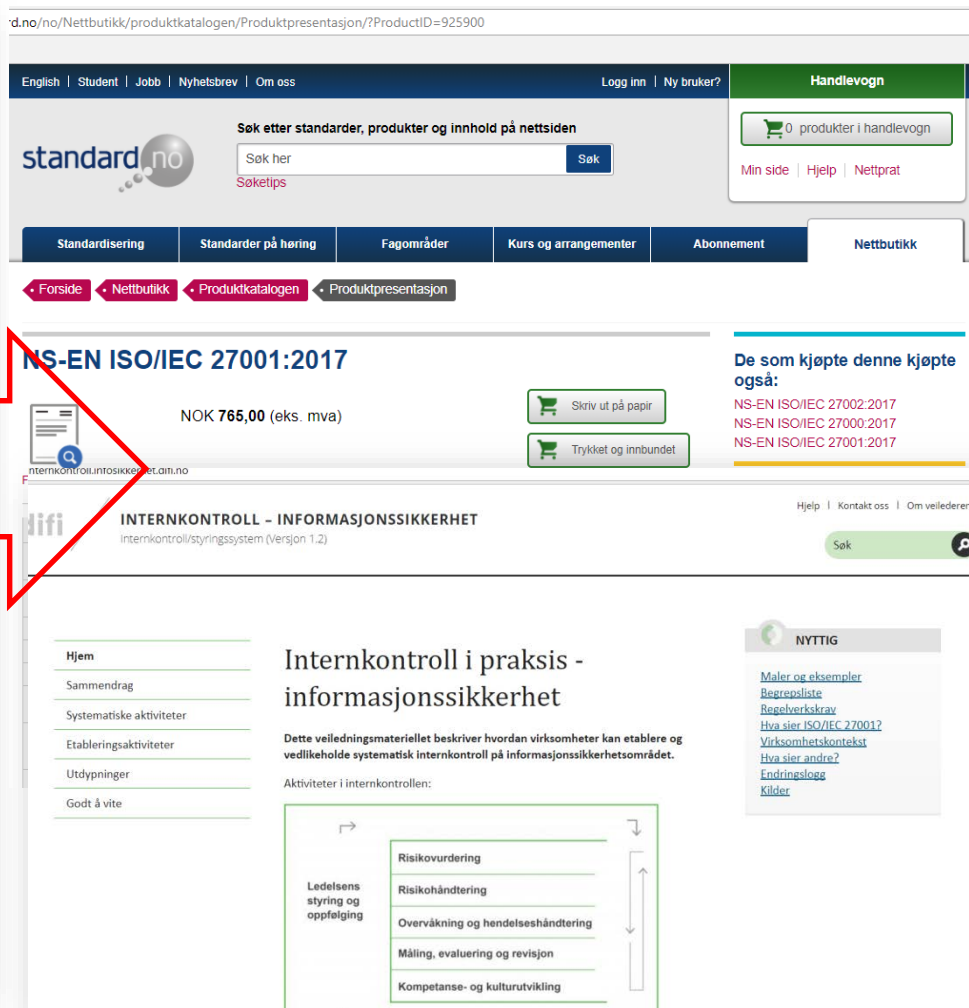
Malene enkeltvis:

- [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?



En veiledning om internkontroll og informasjonssikkerhet



standard.no

Søk etter standarder, produkter og innhold på nettsiden

Søk her

Handlevogn

0 produkter i handlevogn

Min side | Hjelp | Nettpat

Standardisering | Standarder på høring | Fagområder | Kurs og arrangementer | Abonnement | Netbutikk

Forside | Netbutikk | Produktkatalogen | Produktpresentasjon

NS-EN ISO/IEC 27001:2017

NOK 765,00 (eks. mva)

Skriv ut på papir

Trykket og innbundet

De som kjøpte denne kjøpte også:

- NS-EN ISO/IEC 27002:2017
- NS-EN ISO/IEC 27000:2017
- NS-EN ISO/IEC 27001:2017

INTERNKONTROLL - INFORMASJONSSIKKERHET

Internkontroll/styringssystem (Versjon 1.2)

Hjelp | Kontakt oss | Om veilederen

Søk

Hjem

Sammendrag

Systematiske aktiviteter

Etableringsaktiviteter


Utdypninger

Godt å vite

Internkontroll i praksis - informasjonssikkerhet

Dette veiledningsmateriellet beskriver hvordan virksomheter kan etablere og vedlikeholde systematisk internkontroll på informasjonssikkerhetsområdet.

Aktiviteter i internkontrollen:



NYTTIG

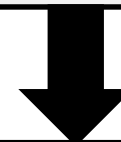
- [Maljer og eksempler](#)
- [Regneark](#)
- [Regelverk](#)
- [Hva sier ISO/IEC 27001?](#)
- [Virksomhetskontekst](#)
- [Hva sier andre?](#)
- [Endringslogg](#)
- [Klikler](#)

Hvilke krav stille GDPR til informasjonssikkerhet?

Virksomheten må etablere "egne" 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



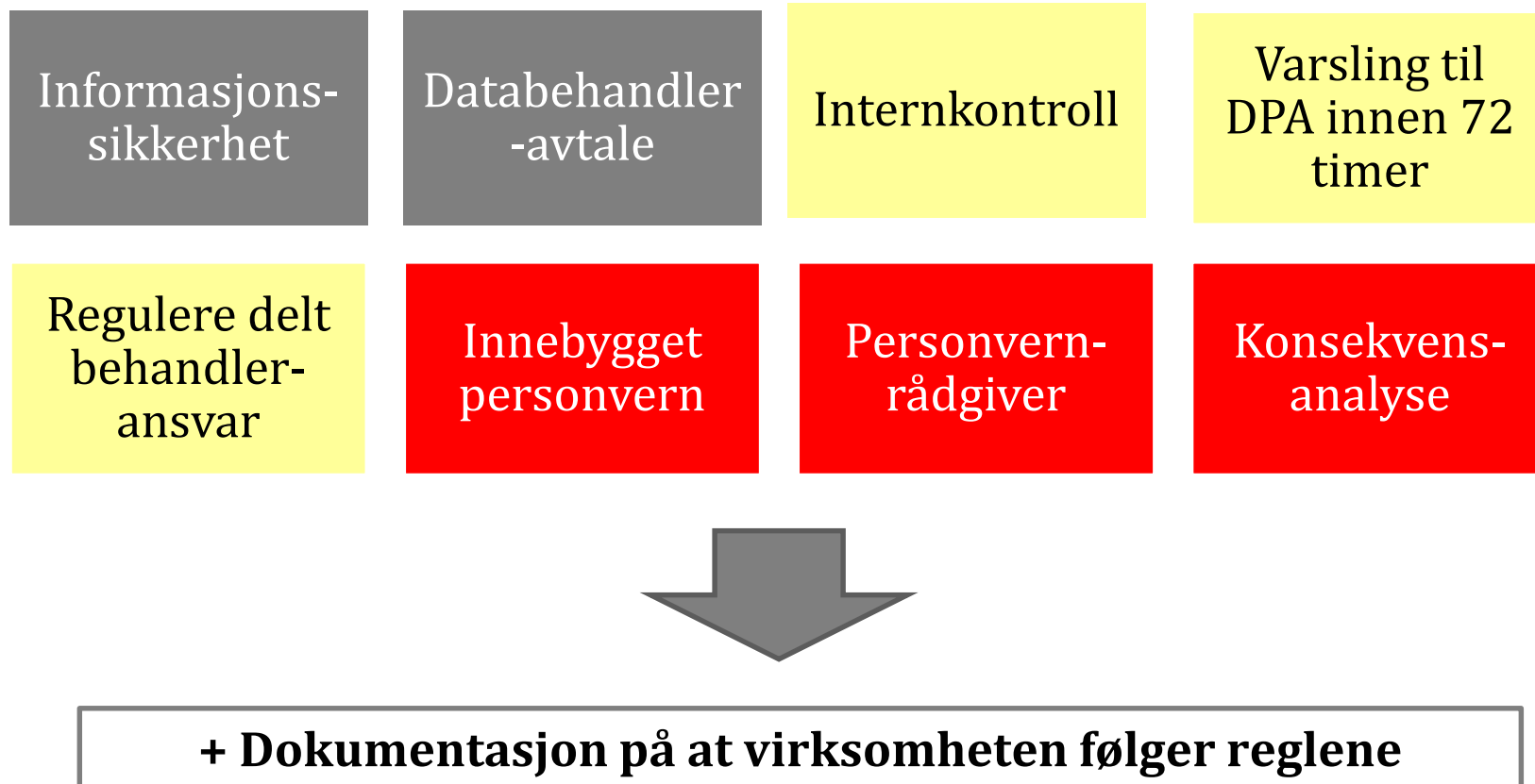
www.identitymanagementinstitute.org

- Personvernrådgiver

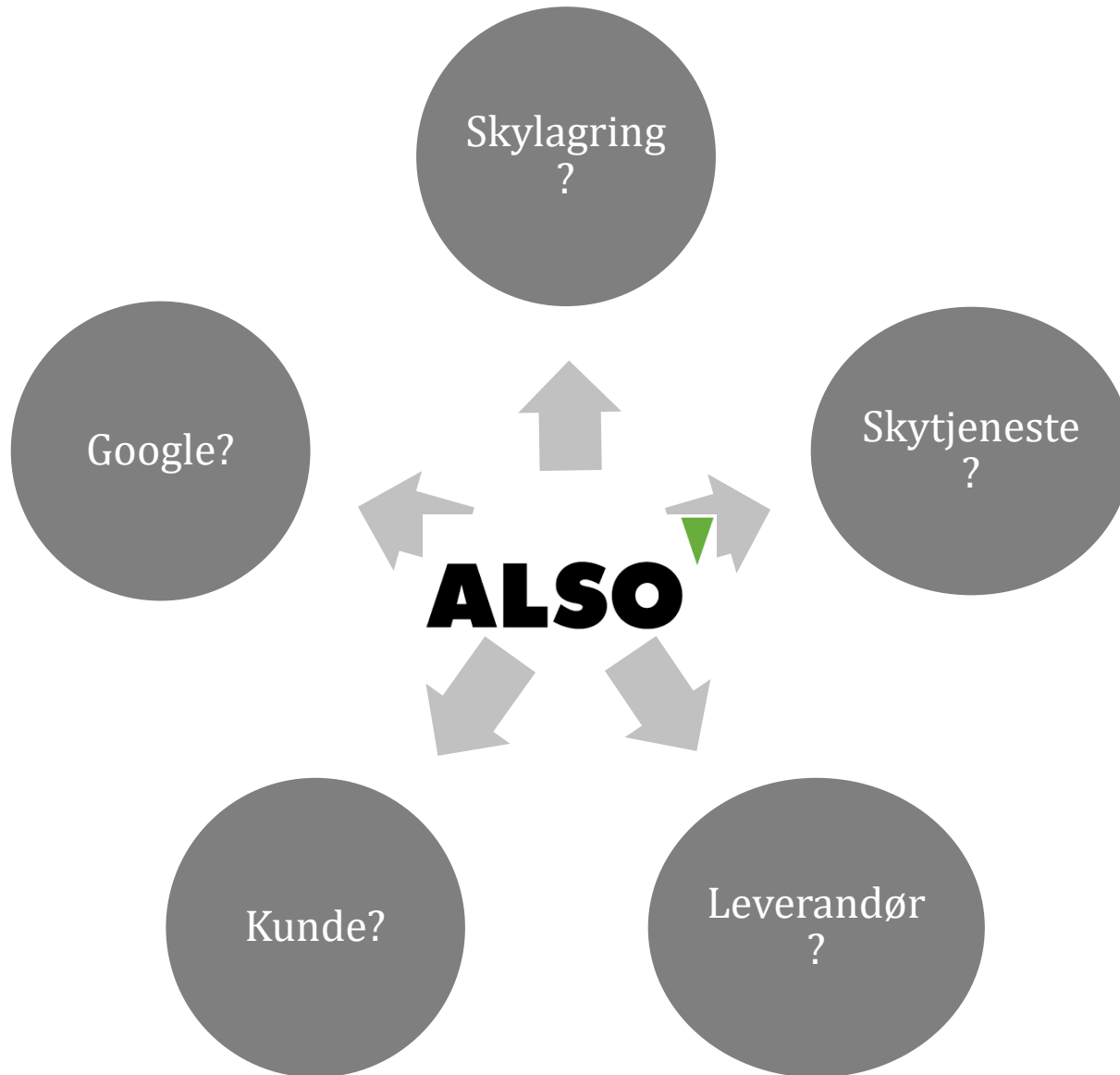


<http://www.cpbuk.co.uk/>

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



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

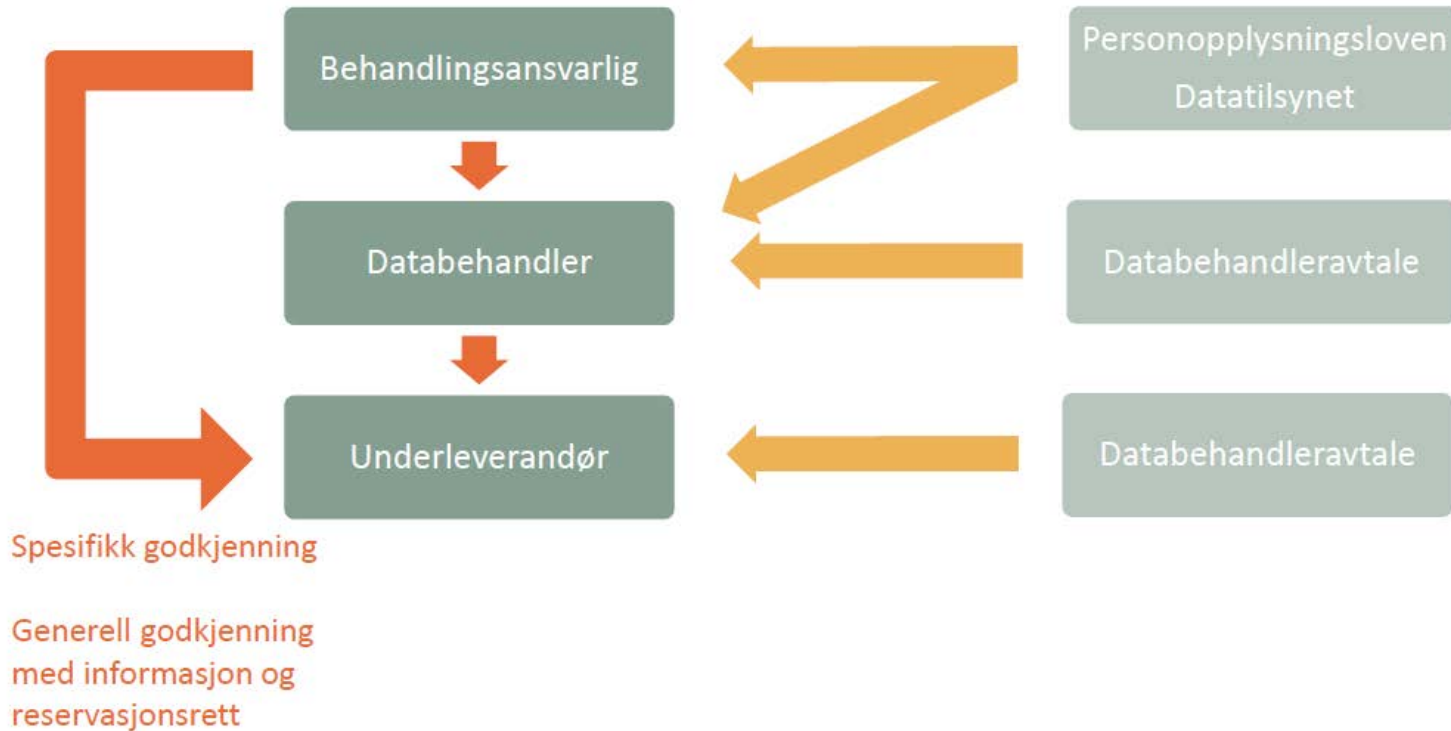
.....
databehandler

Krav til databehandleravtalen

Forordningen stiller følgende krav til innholdet i en databehandleravtale:

- Databehandler skal kun behandle 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.

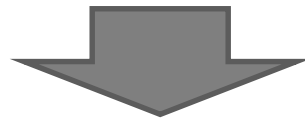
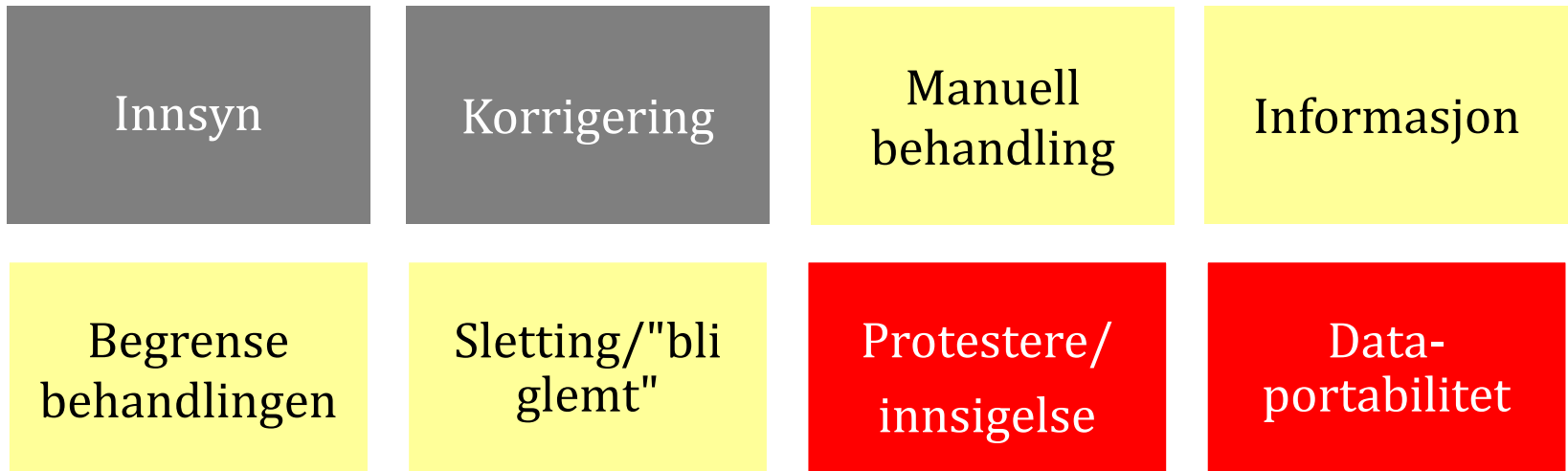
Hva skal databehandleravtalen min inneholde? (3)



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*?



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

The image shows a screenshot of the FINN.no website, which is a real estate and car marketplace. The page displays several listings for cars and houses. A Ghostery browser extension is overlaid on the right side of the page, showing a summary of trackers and blocked items. The extension interface includes a 'Trust Site' button, a 'Restrict Site' button, and a 'Pause' button. A red circle highlights the Ghostery extension and the 'Personvernerklæring' link in the footer.

FINN Mulighetenes marked

Varlinger + Ny annonse Melding

20 000,- Oslo

39 000,- Otta

4 000,- Kalandsvædet

4 750 000,- Noresund

3 450 000,- Bergen

23 500 000,- Oslo

Jobbe i FINN Bli bedriftskunde Admin for bedrifter Native ads Om FINN.no **Personvernerklæring** Cookies Hjelp

Innholdet er beskyttet etter åndsverksloven. Bruk av automatiserte tjenester (roboter, spidere, indeksering m.m.) samt andre fremgangsmåter for systematisk eller regelmessig bruk er ikke tillatt uten eksplisitt samtykke fra FINN.no.

© 1996–2017 FINN.no AS

Ta kontakt hvis du har spørsmål



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

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



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