



SVENSSON
NØKLEBY



Hvem er vi?



Partner Bjørn Jacobsen

Tel: 32 25 55 16

Mob: 936 27 040

E-post: bjacobsen@eurojuris.no



Partner Lene Langseth

Tel: 32 25 55 12

Mob: 950 68 648

E-post: llangseth@eurojuris.no



Det nye personvernregelverket – hva betyr det for din bedrift?

- Hvem er vi?
- **Opplegg:**
 1. Introduksjon
 2. Oversikt over regelverket
 3. Hva må gjøres før 25. mai 2018 og hvordan gjør vi det?

Teneo Data synes IT er gøy

Innspill fra Teneo Data
underveis

Forretningsdrift

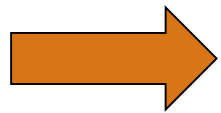
Juss

IT

Motivasjon for arbeidet

- GDPR – høres ut som en diagnose
- Komplisert og omfattende regelverk (31 sider introduksjon, deretter 99 artikler med lovtekst), 100 siders høringssvar fra Datatilsynet
- Mange praktiske spørsmål er overlatt til Artikkel 29-gruppen/ European Data Protection Board (EDPB).
- Krever it-teknisk kompetanse
- Sanksjoner (20 mill Euro eller 4 % global omsetning)
- Kort tid til 25. mai 2018 - kan ikke lenger utsettes

Motivasjonen for arbeidet



Er motivasjonen fryktbasert?

Motivasjonen for arbeidet

- Den enkelte borger ønsker at opplysninger om ham/henne selv beskyttes
- Den enkelte borger ønsker større grad av kontroll
- Den enkelte borger er deg og meg

Motivasjonen for arbeidet

- Respekt for ditt og mitt personvern bør være drivkraften
- God behandling av personopplysninger kan være et konkurransefortrinn?

Ansvarsfraskrivelse

- Stort tema
- Begrenset tid
- Stort spenn av bedrifter / virksomheter
- Konsentrere oss om hovedpunkter / fellesnevner
- Lite rom for nyanser eller særspørsmål
- Trekke ut essensen / forenkle
- Skiller ikke nødvendigvis mellom nyheter og videreføring av dagens regler

DEL 2:


OVERSIKT OVER REGELVERKET



Kort historisk tilbakeblikk

- 1995 EU-personverndirektiv (95/46/EF)
- Direktiv = rammeregelverk med mål, standarder og betingelser
 - ➔ Personopplysningsloven av 14. april 2000
- Vellykket lov, men akterutseilt pga ekstreme endringer i teknologi / bruk av teknologi

1995 til 2018

- Hva gjorde du i 1995?
- 30 mill brukte internett
- Windows 95 lansert, med Internet Explorer som nettleser
-  lansert desember 1995

Formålet med forordningen

- General Data Protection Regulation (GDPR)
 - 1) Sikre borgeres person- og personopplysningsvern
 - 2) Fri utveksling av personopplysninger i EU/EØS

Hvordan innføres forordningen i norsk rett?

- EU-teksten blir norsk lov 25. mai 2018 (henvisningsbestemmelse)
- Dagens personopplysningslov og personopplysningsforskriften oppheves
- Noen tilleggsbestemmelser (f.eks. innsyn e-post og kameraovervåkning i arbeidslivet) innføres / videreføres

Når gjelder forordningen?

- «*Personopplysninger*» =
opplysninger/vurderinger om identifiserbare
mennesker
- «*Helt eller delvis automatisert behandling*» =
Alle former for elektronisk behandling

Når gjelder forordningen?

- Ikke-elektronisk behandling hvis opplysningen skal inngå i et register = strukturert samling av personopplysninger
- Spesiallovgivning vil normalt gå foran personopplysningsloven
- EU arbeider med et ekom-direktiv

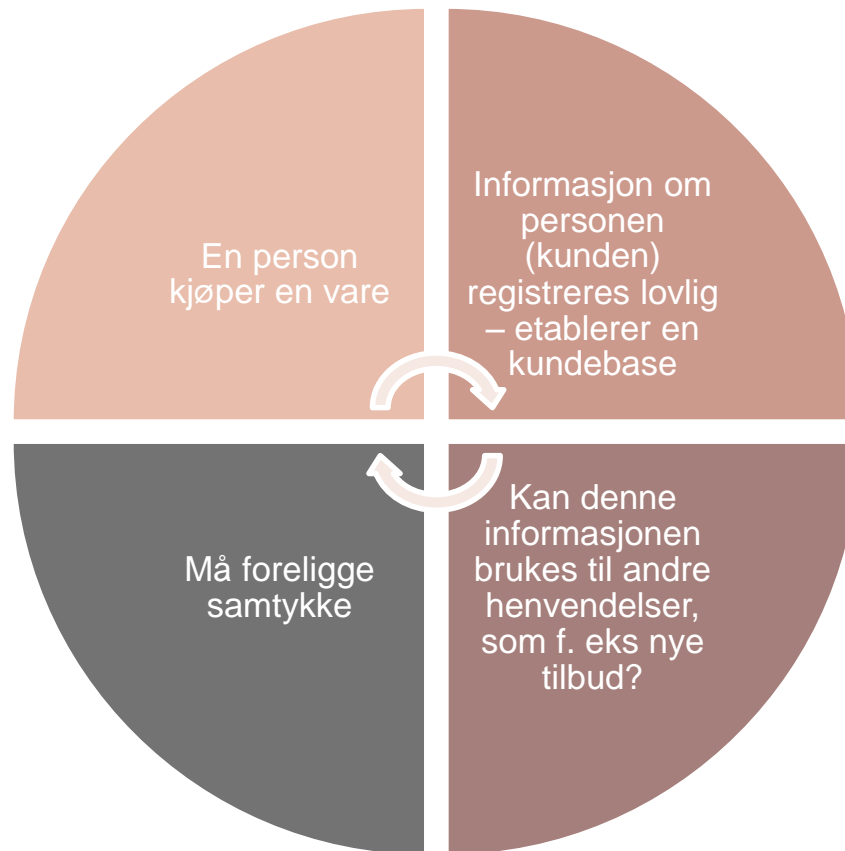
Krav til rettslig grunnlag

- Uttrykkelig angitte og legitime formål
 - Uttrykkelig = veldefinerte
 - Overordnet beskrivelse av formålet er ikke tilstrekkelig
- En rekke generelle rettsgrunnlag

Praktisk viktige rettsgrunnlag

- Samtykke
- Nødvendig for å oppfylle avtale
- Nødvendig for å forfølge en berettiget interesse og hensynet til den registrertes personvern ikke veier tyngre
 - Tenk nøye gjennom hvis dette er behandlingsgrunnlaget

Kjøpssituasjon



Viktige tips til samtykke

- Frivillig
- Spesifikk
- Informert
- Utvetydig erklæring eller klar bekreftelse

Viktige tips til samtykke

- Samtykketekst skal være enkel og forståelig
- Samtykketeksten må være adskilt, f.eks. i standardvilkår
- Samtykke kan ikke være betingelse for tilgang til tjenesten – Må ha reell valgfrihet

Viktige tips til samtykke

- Passive samtykker holder ikke
- NB: Det kreves uttrykkelig samtykke for hver aktuell bruk av personopplysninger
- Det må informeres om at samtykket når som helst kan tilbakekalles
- Samtykket må dokumenteres

Gamle samtykker

- Gamle samtykkeerklæringer er ikke nødvendigvis gode nok

Sensitive personopplysninger

- Sensitive personopplysninger krever særskilt rettsgrunnlag – samtykke ikke nødvendigvis tilstrekkelig

Hva er sensitive opplysninger?

- Etnisk opprinnelse
- Politisk oppfatning, religion, overbevisning eller fagforeningsmedlemskap
- Genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person
- Helseopplysninger eller opplysninger om seksuelle orientering

Hvem retter forordningen seg mot?

- Behandlingsansvarlig
 - Den som bestemmer formålet med behandlingen
 - Og hvilke midler som skal benyttes
- Databehandler
 - Den som behandler personopplysninger på vegne av den behandlingsansvarlige (typisk ekstern it-leverandør eller regnskapsfører)

Databehandleravtaler

- Hvor mange her benytter seg av eksterne tjenester hva gjelder:
 - Regnskapsføring
 - Revisjon
 - Sky-tjenester
 - Web- og serverhotell
 - Faktura- og inkassotjenester
- Hvor mange har en databehandleravtale?

Databehandleravtale

- Nødvendig i de tilfellene hvor du har en databehandler og en behandlingsansvarlig
- Det blir strengere krav til databehandleren og avtale mellom partene
- Databehandlere skal etter det nye regelverket også påse at personvern sikres.

Må databehandleravtalen oppdateres?

- **JA.** Det blir nå strengere krav til databehandlere og databehandleravtalen.
- **Etter dagens regelverk er det f. eks ikke krav til:**
 - At man skal angi hensikten med behandlingen
 - Varigheten av behandlingen
 - Behandlingens formål og art
 - Hvilke opplysninger som skal behandles.
 - Behandlingsansvarliges rettigheter og plikter
 - Varslingsplikt

Overføring ut av EØS

- Hovedregel: kun til stater som garanterer tilfredsstillende beskyttelse
- Flere unntak, bla:
 - Overføring til USA ok forutsatt at amerikansk virksomhet er tilsluttet EU-U.S Privacy Shield avtale
 - Ellers: EU standard overføringsavtaler

Har du tenkt over?



At vi etterlater oss digitale fotavtrykk hele tiden.

Datasystemer og krav til innebygd personvern

- Hva er det?
 - Informasjonssystem som brukes skal oppfylle personvernprinsippene og ivareta de registrertes rettigheter.
 - Det betyr at systemene skal ha et innebygd personvern og personvern som standardinnstilling.
- Hvem er reglene relevant for?
 - For de som utvikler og bidrar til utvikling av programvare som benytter personopplysninger.

Datasystemer og krav til innebygd personvern fortsetter

- Hvorfor er det utarbeidet regler for innebygd personvern?
 - Brukerne forventer at tjenester er sikre og ivaretar personvernet på en god måte.
 - Viktig at de grunnleggende prinsippene for personvern, dvs har man rett til å innhente opplysningene, brukes for bestemte formål og at det kun er opplysninger som er nødvendige som skal innhentes.

Cookies

For å gi deg en bedre opplevelse bruker (navn på virksomheten) vi informasjonskapsler. Ved å fortsette å bla gjennom websiden godtar du vår bruk av informasjonskapsler. Jeg aksepterer dette.



Hva med bedriftens nettsider?

Oppdatering av:

- Personvernerklæringer
- Brukervilkår/standardvilkår
- Samtykketekster

Den enkeltes rettigheter



Rett til informasjon

- Rett til informasjon når opplysninger samles inn fra den enkelte borger
- Rett til informasjon når personopplysninger samles inn fra andre

Hvilken informasjon skal de få?

- Identitet til behandlingsansvarlig og eventuelle representanter
- Formålet med behandling av personopplysninger, samt det rettslige grunnlaget
- Eventuelle mottakere av personopplysninger
- Om personopplysninger skal overføres ut av landet
- Hvor lenge opplysningene vil bli lagret
- Informasjon om at man kan kreve innsyn i hvilke opplysninger som er registrert, korrigere disse eller be om sletting/begrensning i behandlingen.
- Dersom behandlingen er basert på samtykke, at samtykke når som helst trekkes tilbake
- At man har rett til å klage til en tilsynsmyndighet

Rett til innsyn

- Rett til kopi av personopplysningene som behandles

Rett til innsyn

- Unntak:
 - Hemmelighold påkrevd ifm forebygging, etterforskning mv av straffbare handlinger
 - Opplysninger underlagt lovbestemt taushetsplikt
 - Strid med åpenbare og grunnleggende private eller offentlige interesser, herunder hensynet til den registrerte selv
- Unntaket for opplysninger i interne dokumenter videreføres ikke

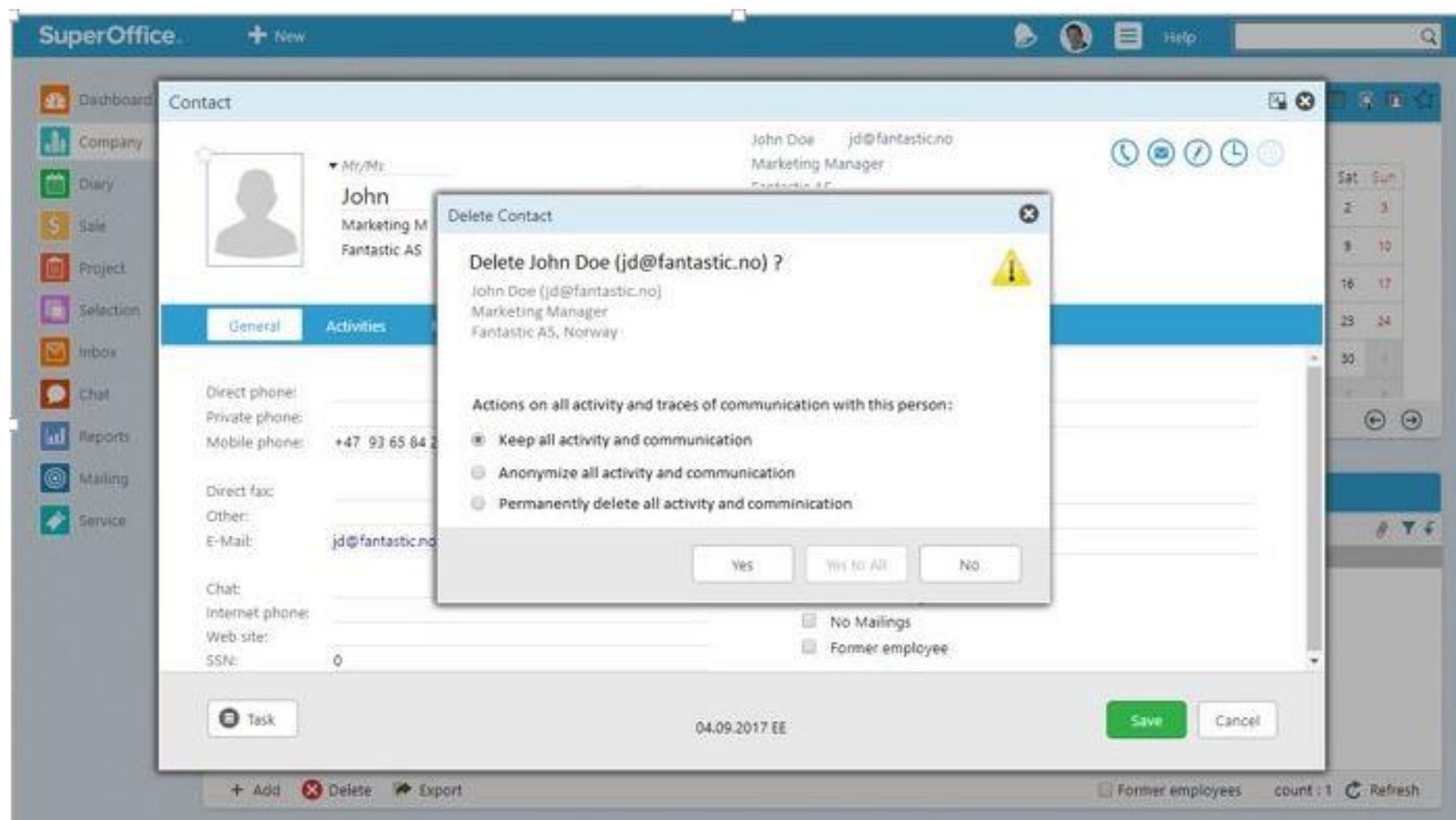
Rett til sletting

- Retten gjelder kun i gitt tilfeller
- To praktiske tilfeller:
 - Personopplysningene ikke lenger er nødvendig for formålet
 - Samtykke er trukket tilbake, ikke annet rettslig grunnlag (f.eks avtale, oppbevaringsplikt eller legitim interesse)

Rett til dataportabilitet

- Rett til å motta personopplysninger i «strukturert, alminnelig anvendt og maskinleselig format»
- Rett til overføring direkte til ny behandlingsansvarlig dersom teknisk mulig
- Reiser en rekke kompliserte spørsmål

Din programvare vil gi deg drahjelp



Protokoll over behandling

- Behandlingsansvarlig bør eller må føre protokoll over behandlingsaktiviteter
 - Ikke egen protokoll for hver enkelt kunde, ansatt eller forbindelse
 - Sett med operasjoner
- Protokoll = dokument / liste
- Benytt word, excel eller spesial software

Protokoll over behandling

- Unntak hvis under 250 ansatte og behandlingen skjer «leilighetsvis»
 - Legg til grunn at protokoll må føres

Protokollens innhold

- Navn og kontaktinfo til behandlingsansvarlig (og eventuelt personvernombud)
- Formålet med behandling
- Beskrivelse av kategoriene av registrerte (borgere) og kategoriene av personopplysninger

Protokollens innhold

- Kategoriene av mottakere
- Opplysninger om eventuell overføring til tredjeland
- Hvis mulig planlagt tidsfrister for sletting
- Hvis mulig generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak

Digitale håndbøker (internkontroll)

Visma Håndbøker

PERSONALHÅNDBOK

fra kr 12,- /mnd./bruker

La de ansatte finne svarene selv.

Les Mer ▾

HMS-HÅNDBOK

fra kr 12,- /mnd./bruker

Alt om HMS samlet på ett sted.

Les Mer ▾

LEDERHÅNDBOK

fra kr 12,- /mnd./bruker

Ivareta dine ansatte med god ledelse.

Les Mer ▾

SYKEFRAVÆRSHÅNDBOK

fra kr 12,- /mnd./bruker

Støtteverktøy for ledere ved sykdom og fravær.

Les Mer ▾

PERSONVERNHÅNDBOK

fra kr 690,- /mnd./firma

Nye personvernreglene trer i kraft mai 2018

Les Mer ▾



Protokoll

- Databehandler også plikt til å føre protokoll
 - Ikke like omfattende

Personkonsekvensutredning (DPIA)

- Ved høy risiko for borgers rettigheter og friheter krav til særskilt utredning
- Typisk:
 - Sensitive data eller data «highly personal nature»
 - Bruk av «big data»
- Konsesjon avskaffet, mulighet for forhåndsdrøfting

Kort om personvernombud

- Hvem må ha personvernombud?
 - Alle offentlige virksomheter
 - Kjerneaktivitet å gjøre følgende i stor skala:
 - Regelmessig og systematisk overvåke personer
 - Behandle sensitive personopplysninger eller opplysninger om straffbare forhold

Kort om personvernombud

- Datatilsynet: Legekontorer og advokater normalt ikke «i stor skala»
- Personvernombud – særlig ressursperson
 - Gi råd, overvåke etterlevelse og være kontaktpunkt
 - «Vaktbikkje»

Avviksrutiner

- Brudd på sikkerhet av et visst omfang
- Filer på avveie, systembrudd, tyveri, passord på avveie, menneskelige feil
- Meldeplikt til Datatilsynet (72 timer)
- Varsling til berørt hvis «høy risiko» (så raskt som mulig)

DEL 3: HVA MÅ GJØRES?



Del 3 – Hva må gjøres før 25. mai?



Hva må gjøres?

- Lederansvar – kan ikke outsources
- Opplæring av ansatte!
- Tekniske grep (datasikkerhet særlig viktig)

Kartlegging

- Kartleggingsmøte
 - Daglig leder, driftssjef, it-ansvarlig og personalansvarlig (typisk)
 - Mange bedrifter kommer langt med en halv dag
 - PS: 18 lørdager igjen før 25. mai 2018
 - PS 2: Kom i gang!

Kartleggingen

- Hvilke teknologier bruker bedriften? I hvilke settinger møter vi mennesker?
 - Hvilke personopplysninger samler vi inn?
 - Hvordan samles de inn?
 - Hva bruker vi de til?
 - Hvor lagres de / sendes de?
 - Hvem har tilgang?
 - Hvor lenge beholder vi opplysningene?

Kartleggingen


- Systematiser «funnene»
 - Word, Excel eller egne spesialprogram
- Har vi et tilstrekkelig behandlingsgrunnlag?

Informasjon/ intern opplæring

Intern Teneo Data AS - GDPR (Internkontroll) | Microsoft Teams

IN Internkontroll > Intern Teneo Data AS - GDPR ☆ ...


Samtaler Filer Wiki +




Se mer

← Svar

12. januar 2018




Ingve Skaret 12.01 14.17
<https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Compliance-Manager-Preview-is-now-available/ba-p/124662>




Compliance Manager Preview is now available
Customers have told us about their compliance challenges, such as the lack of in-house capabilities to define and implement controls, the lack of collaboration between compliance and IT teams, an...
techcommunity.microsoft.com

← Svar



Linda Wang 12.01 14.42
GDPR - Visma og partnere
GDPR - Visma og partnere
Partnere sin rolle og ansvar
Det ligger i GDPR sin natur at hver enkelt bedrift som behandler persondata selv må gjennomgå sine rutiner og sitt kvalitetssystem i forhold til dette. Åpenhet og internkontroll er to nøkkelord. For den Visma programvaren dere

Se mer



Datatilsynet - personvern og informasjonssikkerhet
Datatilsynet skal medvirke til at den enkelte ikke vert krenka gjennom bruk av opplysningar som kan knyttast til han eller henne.
www.datatilsynet.no

← Svar



Hva må gjøres?

- Har vi en god personvernerklæring?
 - Hvor finner brukerne den? Er den lett synlig?
- Har vi en god samtykkeerklæring?
- Har vi oppdaterte databehandleravtaler?
- Lag protokoller for behandling
- Trenger vi et personvernombud? I så fall utarbeid instruks for personvernombudet

Internkontroll

- Personvernpolicy som en del av internkontrollsystemet
 - Sletterrutiner
 - Innsynsrutiner
 - Datasikkerhetsrutiner
 - Rutiner for DPIA ved bruk av ny teknologi?
 - Avviksrutiner

- Dokumenter arbeidet virksomheten gjør frem til 25. mai (og videre)

AKTUELLE LINKER

- Norsk uoffisiell oversettelse:

<https://www.datatilsynet.no/globalassets/global/regelverk-skjema/forordningen/uoffisiell-norsk-oversettelse-av-personvernforordningen.pdf>

- Engelsk tekst:

<http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL>

Datatilsynets veileder:

<https://www.datatilsynet.no/regelverk-og-skjema/veiledere/hva-betyr/>



Erfaring. Kompetanse. Løsning.

