SVENSSON
NØKLEBY

Hvem er vi?

Advokat Bjørn Jacobsen

Tel: 32 25 55 16
Mob: 936 27 040
E-post: bjacobsen@eurojuris.no

Advokatfullmektig
Liv-Astrid Rustgaard Bjerke

Tel: 32 25 55 06
Mob: 920 62 928
E-post: lrustgaardbjerke@eurojuris.no

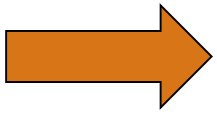
Det nye personvernregelverket – hva betyr det for din bedrift?

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

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).
- Sanksjoner (20 mill Euro eller 4 % global omsetning)
- Kort tid til 1. juli 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 / fellesnevnere
- 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

Hovedelementer

- «Sikkerhetsnivå som er egnet i forhold til risiko»
  - *«security, integrity and confidentiality»*
  - Krav til tekniske tiltak
  - Krav til organisatoriske tiltak
- Større grad av bevissthet
  - *«transparancy, fairness and lawfulness»*
- Streng dokumentasjonsplikt

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

Alminnelige personopplysninger (ikke uttømmende)		
Navn	Andre registreringer av en persons bevegelser på nett	Opplysninger om utleggstrekk
Personnummer	Påloggінger i datasystemer	Bilnummer
Stilling	Opplysninger fra adgangskontroll	IP-adresse
Adresser	Opplysninger om pårørende og barn	Bilder
Telefonnummer	Bankkontonummer	Opplysninger om adferdsmønster
E-post		

Når gjelder forordningen?

Sensitive personopplysninger
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

Når gjelder forordningen?

- Ikke-elektronisk behandling hvis opplysningen skal inngå i et register = strukturert samling av personopplysninger

- Spesiallovgivning vil normalt gå foran personopplysningsloven

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

Sensitive personopplysninger

- Sensitive personopplysninger krever særskilt rettsgrunnlag – samtykke ikke nødvendigvis tilstrekkelig

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

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.

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.**

- Reguleres av lov om elektronisk kommunikasjon
- GDPR kan få betydning
- EU arbeider med et ekom-direktiv

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.

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 kun delvis.

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

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

Eksempel / utgangspunkt

Dataansvarlig	**Navn på bedrift +kontaktopplysninger (adresse, hjemmeside, telefonnummer, e-post)**	**XXXXXX AS Fyll inn**
	Behandlingsansvarlig + kontaktopplysninger	Daglig leder YYYYY Fyll inn
	Personvernombud	Ikke aktuelt
Formål (-ene)	Behandlingens formål (hvorfor behandles opplysningen?)	Personaladministrasjon og rekruttering
Kategori av registrerte og type personopplysninger	Kategori av registrerte (eksempelvis borgere, kontaktpersoner hos kunder/leverandører, søkere, ansatte, tidligere ansatte)	Personopplysninger behandles for følgende kategorier: a) Søkere b) Ansatte c) Tidligere ansatte d) Pårørende til ansatte e) Fyll inn
	Opplysninger som behandles	• Identifikasjonsopplysninger, herunder fødselsnummer • Kontaktinformasjon • Bilde • CV • Informasjon om utdannelse og kurs • Opplysninger om arbeidsforholdet til bruk for administrasjonen. Herunder: Stillingskategori, lønnsopplysninger, skattetrekksopplysninger, sykefraværsopplysninger, medarbeiderreferater, advarsler m.m. • Fagforeningsmedlemsskap (kun til bruk for fagforeningskontigentstrekk samt i forbindelse med informasjonsutveksling med klubb og fagforening • Fyll inn

Mottakere av personopplysninger	**Kategorier av mottakere som opplysningene sendes til eller utveksles med (eksempelvis myndigheter, virksomheter, borgere, foreninger etc)**	• **Offentlige myndigheter (typisk skattemyndigheter og NAV)** • **Banker** • **Pensjonsleverandør** • **Forsikringsmegler og forsikringsselskap** • **Leverandører av datasystemer (kun som del av normal drift av systemer)** • **Kunder og leverandører (kontaktinformasjon)** • **Fyll inn**
Tredjeland og internasjonale organisasjoner	Opplysninger om overførsel av personopplysninger til utenfor EØS eller til internasjonale organsiasjoner	• Ikke aktuelt
Sletting	Tidspunkt for sletting av opplysninger (forventet tidsfrister for sletting av ulike kategorier opplysninger)	• Opplysninger om søkere slettes senest X måneder etter at rekrutteringsprosess er avsluttet (hvis ikke uttrykkelig samtykke til lagring er innhentet) • Opplysninger om tidligere ansatte slettes 12 måneder etter at arbeidsforholdet er avsluttet, likevel slik at identifikasjonsopplysninger, kontaktinformasjon og opplysninger om tittel, lønn samt andre opplysninger som er nødvendig å oppbevare som følge av arbeidsforholdet vil bli oppbevart videre. •
Tekniske og organisatoriske sikkerhetstiltak	Generell beskrivelse av tekniske og organisatoriske sikkerhtstiltak	• Behandling av personopplysninger skjer i samsvar med interne retningslinjer. Innebærer blant annet at tilgang til informasjon er begrenset til spesifikke personer. • Fødselsnummer benyttes kun der det er nødvendig av hensyn til sikker identifisering. Lønnsslipp med fødselsnummer i lukket konvolutt / kryptert e-post, via portalløsning eller i anonymisert form (stryk det som ikke passer) • Inntatt retningslinjer for personvern i personalhåndbok samt intranett • Papirdokumenter oppbevares i låst skap • Oppdatert it-plattform med relevante oppdatert sikkerhetsprogramvare • Eventuelle sertifiseringsordninger: ISO XXXX

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: 6 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?

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
  - Sletterutiner
  - Innsynsrutiner
  - Datasikkerhetsrutiner
  - Rutiner for DPIA ved bruk av ny teknologi?
  - Avviksrutiner

- Dokumenter arbeidet virksomheten gjør frem til 1. juli 2018 (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.