



Ole Bjørn Nordland, rådmannens fagstab, november 2017

EUs personvernforordning (GDPR)



Hva er personvern?



Regjeringen.no:

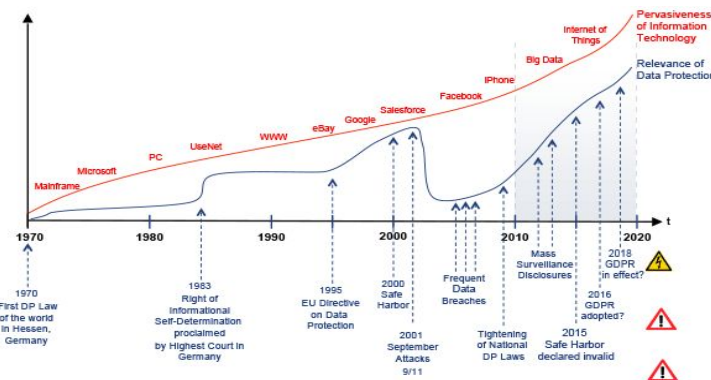
Personvern handler om retten til å få ha ditt privatliv i fred, et grunnleggende prinsipp i en rettsstat.

Idealet er at den enkelte skal ha råderett over sine egne personopplysninger.

Litt historikk:

- Diverse internasjonale konvensjoner:
(Menneskerettighetene 1948, Menneskerettskonvensjonen 1950, FN-konvensjonen 1966, Barnekonvensjonen 1989)
- Personregisterloven (1978)
- Personopplysningsloven (2001)
- EUs personverndirektiv (1995)
- EUs personvernforordning (2016)
- Grunnlovens § 102 (2014)
- Ny personopplysningslov m. forskrifter - 25. mai 2018(?)
(Forordningen, høringsnotat, utkast til ny lov - se ["regjeringen.no"](https://www.regjeringen.no))

"The Right to Privacy" (1890)



EU GDPR

- Vedtatt i april 2016, trer i kraft 25. mai 2018
- I Norge; medfører ny personopplysningslov med forskrift(er)
- endringer i eksisterende lover



EU GDPR - oppbygging

- Felles lov i EU/EØS

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 the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- 173 forutsetninger/
anbefalinger/prinsipper

- 11 kapitler, 99 artikler -
1021 krav/pålegg

What the new EU GDPR means in 1 minute

The EU GDPR will increase privacy for individuals and give regulatory authorities greater powers to take action against businesses that breach the new laws. Here's what it means for your business:

Tough penalties: fines of up to **4%** of annual global revenue or **€20 million**, whichever is greater.

The regulation also applies to **non-EU companies** that process personal data of individuals in the EU.

The **international transfer of data** will continue to be governed under EU GDPR rules.

The **definition of personal data** is now broader and includes identifiers such as:

- genetic
- mental
- cultural
- economic
- social identity.

Obtaining consent for processing personal data must be clear, and must seek an affirmative response.

Data subjects have the **right to be forgotten** and erased from records.

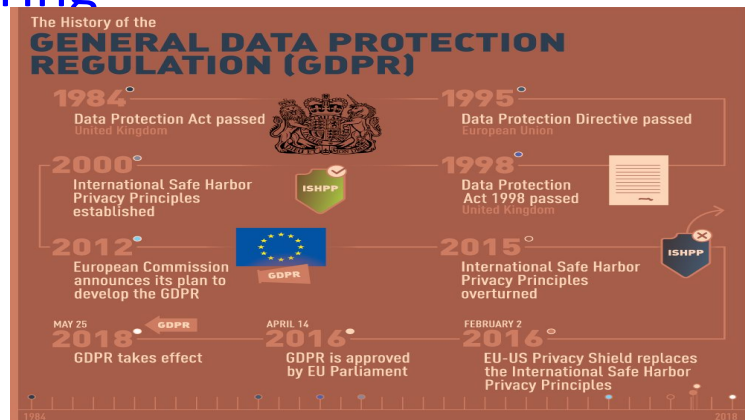
Parental consent is required for the processing of **personal data of children** under age 16.

Users may request a copy of personal data in a **portable format**.

EU GDPR - forskjeller fra tidligere

Hovedforskjeller fra før:

- Større geografisk virkeområde
- Strengere straffer
- Strengere krav til behandlingsgrunnlag (consent)
- Strengere krav til avviksrapportering
- Enklere tilgang til egne data
- Krav til å kunne bli glemt
- Krav til dataportabilitet
- Krav til innebygd personvern
- Krav om personvernombud



EU GDPR - innramming

- Gjelder for alle virksomheter/firma med tilhold i **EU/EØS**, eller som behandler personopplysninger fra EU-borgere
- Gjelder **all behandling** av personopplysninger som påvirker den registrertes rettigheter eller friheter
- **Ansvar og roller**: databehandlingsansvarlig, databehandler, og personvernombud
- Dokumentere **etterlevelse** 25. mai 2018



EU GDPR - ansvar og kostnader

- **DBA/Controller** og **DB/Processor** er sammen ansvarlig for avvik eller manglende etterlevelse
- **PVO/Data Protection Officer** skal gi råd/utøve kontroll
- “tilstrekkelig sikkerhet” - ikke definert
- Straff: 20 mill Euro/4% brutto(GAT)
- PwC: (US) 70% - \$ 1-10 mill, 10% -\$10+ mill
- Ovum: (US) 50% er forberedt på bøter (non-compliance)
-  Oliver Wyman: \$6 mrd i bøter - første år

EU GDPR - overordnet prinsipp

Pkt 1: Vern av fysiske personer i forbindelse med behandling av personopplysninger er en grunnleggende rettighet. (...)



EU GDPR - definisjoner

I dag:

Personopplysning - Pol. §2.1 (jf art 2)

opplysninger og vurderinger som kan knyttes til en enkeltperson

Personopplysning er en opplysning eller vurdering som kan knyttes til deg som enkeltperson, slik som for eksempel navn, adresse, telefonnummer, e-postadresse, *IP-adresse*, bilnummer, bilder, fingeravtrykk, irismønstre, hodeform (for ansiktsgjenkjenning) og fødselsnummer (både fødselsdato og *personnummer*).

Opplysninger om atferdsmønstre er også regnet som personopplysninger. Opplysninger om hva du handler, hvilke butikker du går i, hvilke tv-serier du ser på, hvor du beveger deg i løpet av en dag og hva du søker etter på nettet er alt sammen personopplysninger. En av de nyere utfordringene for personvernet er at vi legger igjen så mange digitale spor. Disse opplysningene utnyttes ofte kommersielt uten at du har samtykket til det.

Sensitiv personopplysning - Pol. §2.8 (jf art 9, og 10)

opplysninger om rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning, at en person har vært mistenkt, **siktet, tiltalt eller dømt for en straffbar handling**, helseforhold, seksuelle forhold eller medlemskap i fagforeninger.

Fra 25.mai 2018:

Med forbehold - Omtrent som i dag!

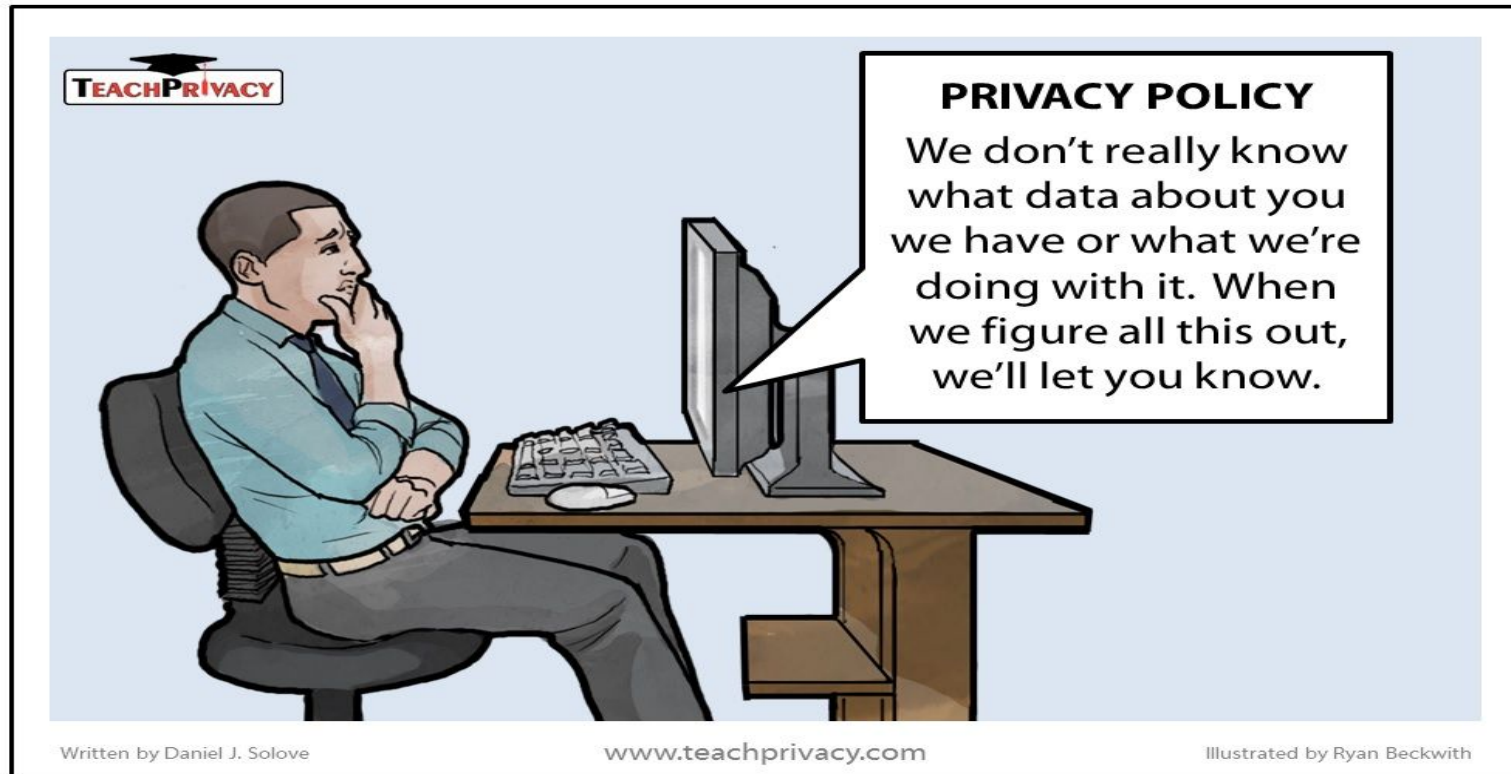
EU-domstolen har avgjort at dynamiske IP-adresser i gitte tilfeller skal regnes som personopplysninger
Genetiske og biometriske opplysninger med formål å entydig identifisere en fysisk person blir sensitiv pol.

Hva “treffer oss” i Tk?



- Nye plikter - utfordrer grunnlag og etterlevelse (lovlighet)
- Vurdere risiko- og personvernkonsekvenser
- Krav om innebygd personvern i nye system
- Personvernombud
- Gjelder også for skytjenester utenfor EU/EØS
- Databehandlere får nye plikter/databehandleravtaler
- Anbefaling om bransjenormer
- Nye og strengere krav til avvikshåndtering
- Vi må kunne oppfylle “de registrertes” rettigheter
-  Personvernklæring

Personvernerklæring - ikke slik!



Hva med arkiv?

- GDPR Artikkel 9, nr 2, bokstav j.
hjemmel for arkivering av sensitive personopplysninger)
- Høringsnotatet pkt 8.3.6 (og 8.3.7)
arkivformål, forskning og statistikk



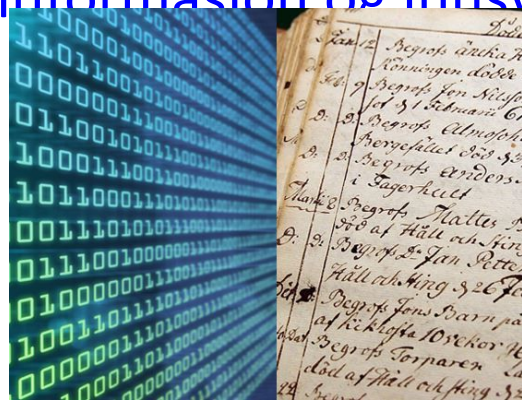
- Lovutkastet § 6,

-”Forbudet i personvernforordningen artikkel 9 nr. 1 gjelder ikke i den utstrekning behandlingen er nødvendig for arkivformål i allmennhetens interesse, ...dersom det er fastsatt i...eller i medhold av lov, eller dersom... a) uforholdsmessig vanskelig... b) klart overstiger ulempene... c) særlige tiltak for



Hva med arkiv? - forts.

- Lovutkastet § 9. **Bruk av fødselsnummer o.l.**
- Lovutkastet § 11. **Forhåndsdrøfting/ -godkjenning mm.**
- Lovutkastet § 13. **Unntak fra retten til informasjon og innsyn ved taushetsplikt, mm.**
- Lovutkastet § 14. **Unntak fra den registrertes rettigheter ved behandling av personopplysninger for arkivformål mm.**



Hva betyr det for oss personlig?

Forsterket rett til å råde over egne data:

- Utvidet **rett til innsyn** i egne persondata
- Utvidet **rett til å rette** egne persondata
- Retten til **å ta med seg** egne persondata
- Rett til **slette** egne persondata/ “bli glemt”
- Henvendelser skal besvares innen en måned

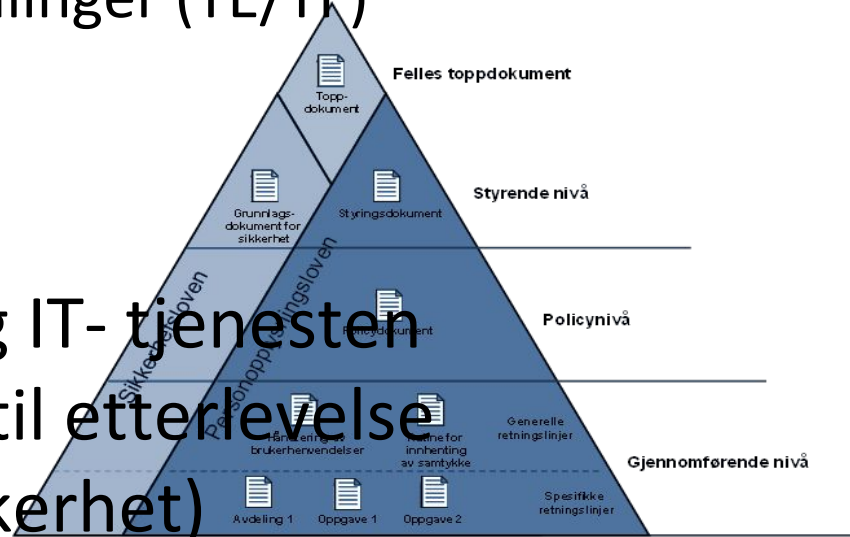


Hva gjør vi?

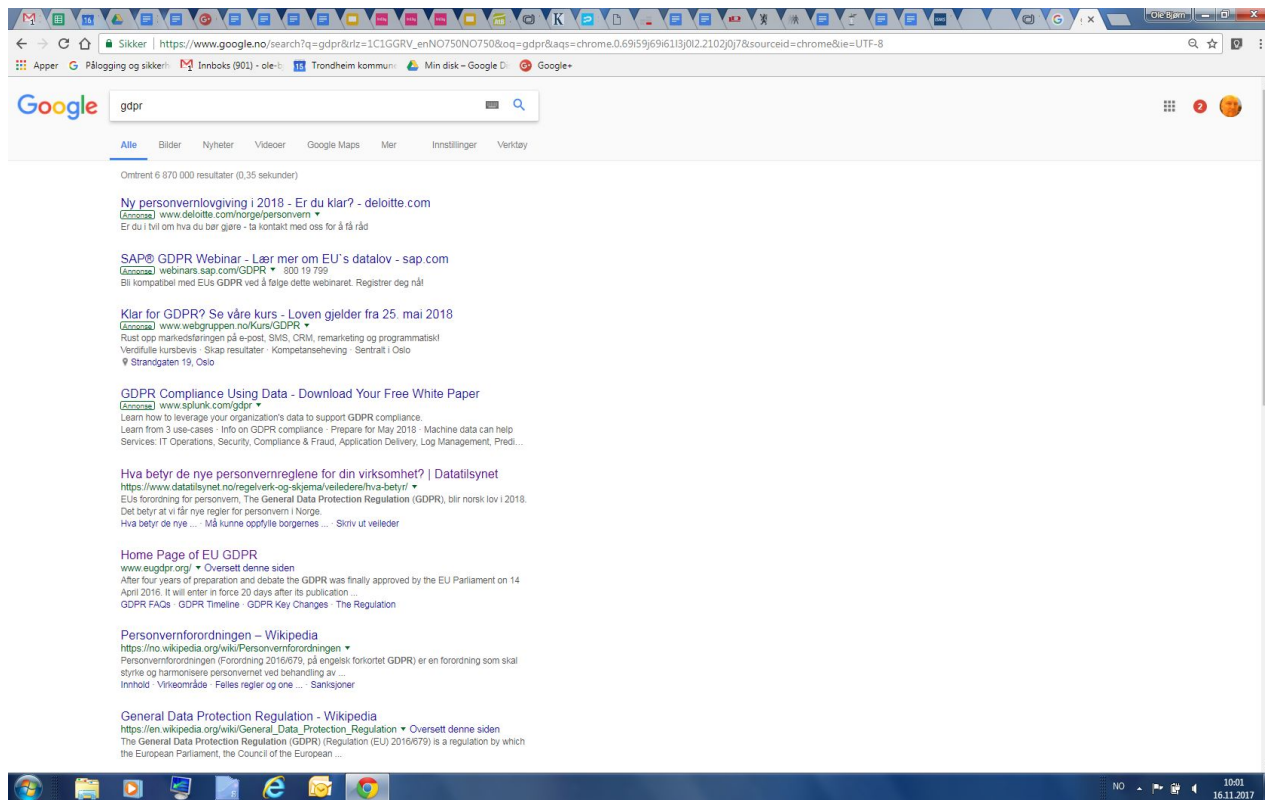
- Prosjekt personvernforordningen
 - Meg, Victor, Ketil A, Tom A, Maria, Arnstein, + direktører/enhetsledere, og Klæbu (Rune/Gunhild)
 - Fase 1: Kartlegging av behandlinger (TE/TF)
 - Fase 2: Lovlighet (TE/TF)
 - Fase 3: Kunnskap (alle)
 - Fase 4: Rutiner (alle)

■ Innebygd personvern: DF og IT- tjenesten

■ Anskaffe verktøy for støtte til etterlevelse (fagsystem informasjonssikkerhet)



Finne info - på nettet?



Home Page of EU GDPR

The screenshot shows the homepage of EUGDPR.org in a web browser. The browser's address bar displays 'www.eugdpr.org'. The website has a dark blue header with navigation links: 'EUGDPR.org', 'The Regulation', 'The Process', 'More Resources', and 'Our Partners'. On the left side, there is a vertical social media bar with icons for Google+, Facebook, Twitter, and a plus sign for more options. The main content area features a large banner with a blue background and yellow stars, resembling the European Union flag. The banner text reads: 'The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years - we're here to make sure you're prepared.' Below this, a countdown timer shows 'TIME UNTIL GDPR ENFORCEMENT UTC' with a digital display of '189:15:01:13' and labels for 'Days', 'Hrs', 'Mins', and 'Secs'. The page is divided into two columns. The left column is titled 'GDPR Portal: Site Overview' and contains a paragraph stating the website's purpose, a paragraph about the GDPR's approval and enforcement date (25 May 2018), and a paragraph about the regulation replacing the Data Protection Directive 95/46/EC. The right column is titled 'Quick Links' and contains two links: 'GDPR Key Changes' (Summary of key changes) and 'FAQs' (How to prepare?, Is my organization affected?, What does Brexit mean for GDPR?). The browser's taskbar at the bottom shows various application icons and the system clock indicating 09:58 on 16.11.2017.

www.eugdpr.org

EUGDPR.org The Regulation The Process More Resources Our Partners

The EU General Data Protection Regulation (GDPR) is the most important change in data privacy regulation in 20 years - we're here to make sure you're prepared.

TIME UNTIL GDPR ENFORCEMENT UTC
189:15:01:13
Days Hrs Mins Secs

GDPR Portal: Site Overview

This website is a resource to educate the public about the main elements of the General Data Protection Regulation (GDPR)

After four years of preparation and debate the GDPR was finally approved by the EU Parliament on 14 April 2016. It will enter in force 20 days after its publication in the EU Official Journal and will be directly application in all members states two years after this date. Enforcement date: 25 May 2018 - at which time those organizations in non-compliance will face heavy fines.

The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. The key articles of the GDPR, as well as information on its business impact, can be found throughout this site.

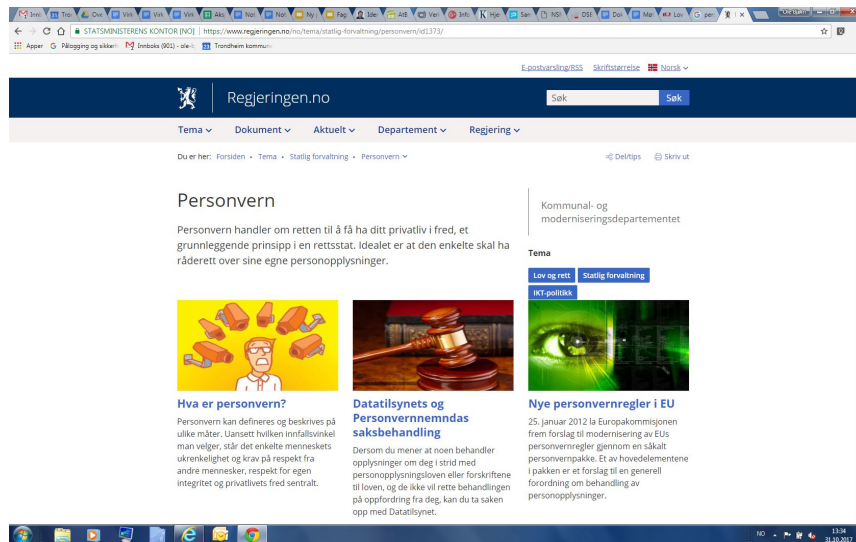
Quick Links

GDPR Key Changes
Summary of key changes

FAQs
How to prepare?
Is my organization affected?
What does Brexit mean for GDPR?

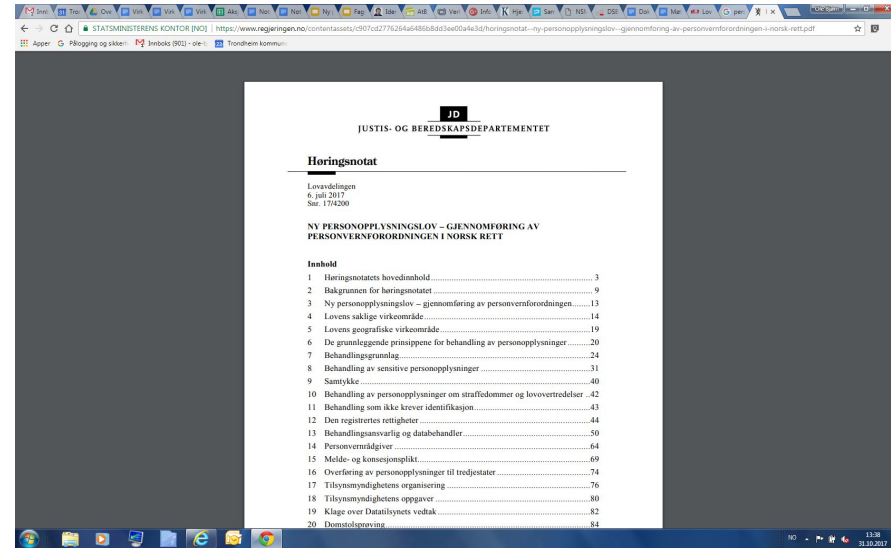
Regjeringen.no

<https://www.regjeringen.no/no/tema/statlig-forvaltning/personvern/id1373/>



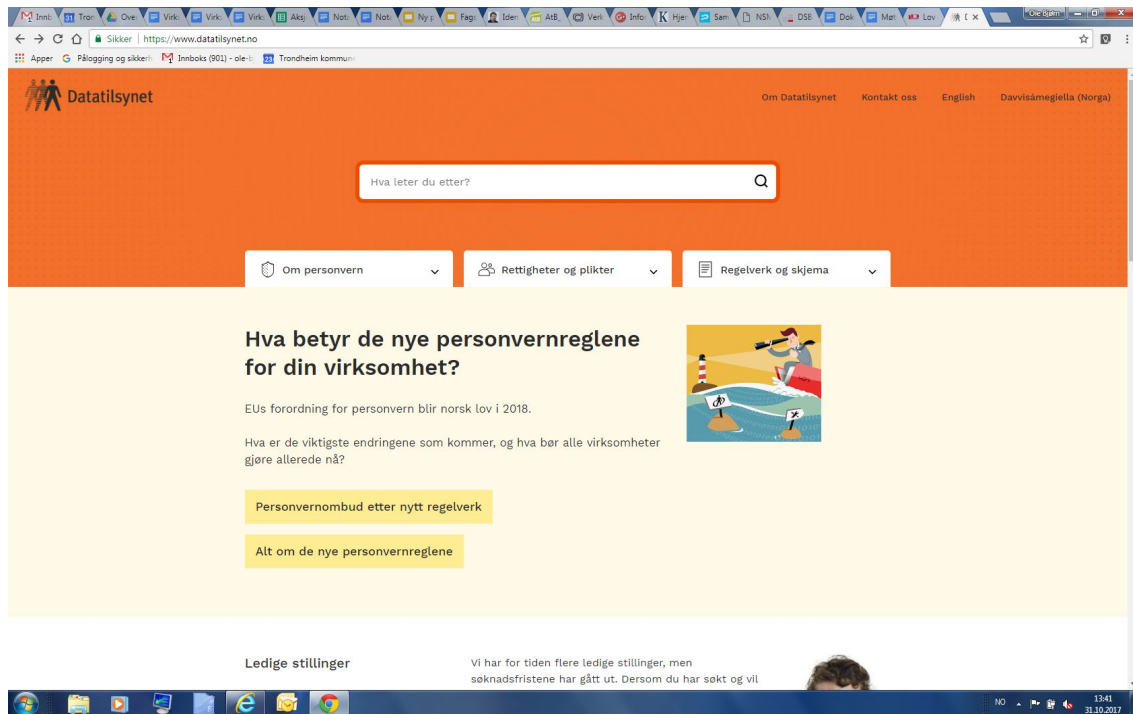
Regjeringen.no

<https://www.regjeringen.no/no/no/dokumenter/horing-om-utkast-til-ny-personopplysningslov--gjennomforing-av-personvernforordningen-i-norsk-rett/id2564300/>



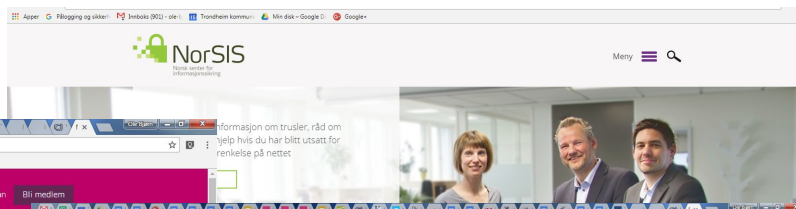
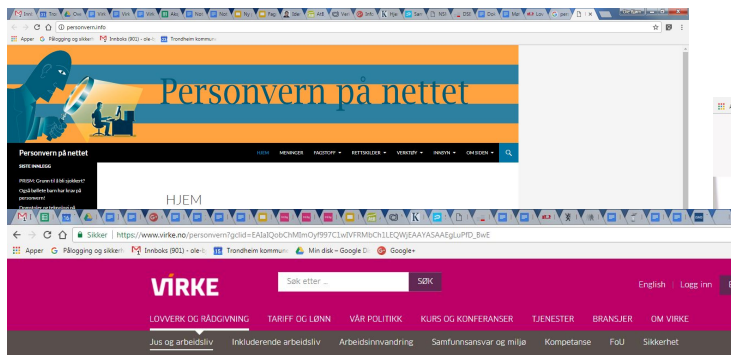
Datatilsynet.no

<https://www.datatilsynet.no/>



The screenshot shows the homepage of the Norwegian Data Protection Authority (Datatilsynet). The website has an orange header with the logo and navigation links: "Om Datatilsynet", "Kontakt oss", "English", and "Datavisningsregler (Norge)". A search bar with the placeholder text "Hva leter du etter?" is centered in the header. Below the header, there are three dropdown menus: "Om personvern", "Rettigheter og plikter", and "Regelverk og skjema". The main content area features a large article titled "Hva betyr de nye personvernreglene for din virksomhet?" (What do the new data protection rules mean for your business?). The article text states: "EUs forordning for personvern blir norsk lov i 2018. Hva er de viktigste endringene som kommer, og hva bør alle virksomheter gjøre allerede nå?" (The EU's regulation for data protection becomes Norwegian law in 2018. What are the most important changes that are coming, and what should all businesses do already now?). To the right of the text is an illustration of a person in a red hat and life preserver floating in the water, with a lighthouse beam shining on them. Below the article text are two yellow buttons: "Personvernombud etter nytt regelverk" and "Alt om de nye personvernreglene". At the bottom of the page, there is a section titled "Ledige stillinger" (Vacancies) with the text: "Vi har for tiden flere ledige stillinger, men søknadsfristene har gått ut. Dersom du har søkt og vil" (We currently have several vacancies, but the application deadlines have passed. If you have applied and want). The website is displayed in a browser window with a Windows taskbar at the bottom showing the date 31.10.2017 and time 13:41.

UiO, Norsis, Virke, osv...



Du er her: Startiden / Lovverk og rådgivning / Jus og arbeidsliv / Personvern

Fagartikler
Faktaark
Lovnytt
Spørsmål og svar
Arbeidslivshåndbok



Nye regler om personvern

Er du usikker på hva det nye regelverket om behandling av personopplysninger betyr for din bedrift? Virke vil publisere informasjon om hva du bør gjøre for å være forberedt før reglene trer i kraft i mai 2018.

For å sikre at din virksomhet er godt nok forberedt, anbefaler vi at du følger Virkes 7 steg mot nye personvernregler. Disse finner du øverst til høyre på denne siden.

Hvem gjelder de nye reglene for?

De aller fleste virksomheter, uavhengig av bransje, behandler og lagrer opplysninger om sine kunder, brukere, pasienter eller ansatte. De nye personvernreglene gjelder for alle virksomheter som i liten eller stor grad behandler personopplysninger.

Hva betyr de nye personvernreglene for din virksomhet?

Bli klar i tide - følg Virkes 7 steg:

- 1 Kartlegg hvilke personopplysninger du behandler
- 2 Sikre at behandlingene er lovlige
- 3 Utarbeid en klar og forståelig personvernerklæring
- 4 Oppdater rutiner for internkontroll
- 5 Oppdater rutiner for informasjonssikkerhet
- 6 Vurder om du må ha personvernombud
- 7 Sikre lovlig overføring data

Nye personvernregler

Du bestemmer.no

- om personvern, nettrett og digitalt demokrati

Yngre barn: 9-13 år 13-18 år Voksne Helse og Elsker Om Du bestemmer

Personvern Sosial på nett Utenlandske hendelser Digitale spør

Personvern

Vi har alle noe vi ikke ønsker å dele med andre. Ikke fordi det er kaiminelt eller noe vi nødvendigvis må skjule, men rett og slett fordi det er privat. Derfor er det også du som bestemmer hva folk skal få vite om deg, og hvilke opplysninger du vil holde for deg selv.



Sjekk artikkelen

Personvern er en grunnleggende rettighet som betyr at du har rett til privatliv og til å kunne bestemme over dine egne personopplysninger. Du skal selv kunne bestemme hvilke opplysninger om deg du vil dele, og med hvem. Når du blir født er det disse foresatte som bestemmer over personopplysninger og hvordan de brukes, men etter hvert som du blir eldre skal dine egne meninger om personvern telle mer.

Krav på privatliv

Selv om du tenker at du ikke har noe å skjule, har du krav på et privatliv. Behovet for å ha en rom for seg selv som andre respekterer og ikke bryter seg inn i, varierer fra person til person. Men synes det er greit å dele mye, mens andre er mer tilbakeholdne. Forskjellige venningsgrupper eller forskjellige kulturer kan ha ulike syn på hva som er greit og hva som kan dele. Dessuten har opplysninger en tendens som er privat ender seg gjennom tid. Det blir fordelt eller befinde seg på så som svart sprø, vil du kanskje dele med venner eller andre.

Vi har alle noe vi ikke ønsker å dele med andre. Ikke fordi det er galt eller usensibelt, men fordi vi ikke ønsker at andre skal vite om det. Det kan være følelser, tanker eller meninger om helse, seksualitet, religion, politikk eller lignende. Jo mer digitalisert hverdagen vår blir, og jo flere opplysninger som

Gruppe og samling på Google+

