Formål med GDPR (The EU General Data Protection Regulation)

- **Harmonisering:**
- Ensartet anvendelse og håndhævelse af databeskyttelsesregler
- Ønske om et digitalt indre marked

- **Styrke borgernes retsstilling:**
- Styrke borgernes retsstilling og beskytte deres frihedsrettigheder ...
- ... ved at styrke krav til **sikkerhed** og **indsigtsmuligheder**

- **Samlet set:**
- Skabe en bedre **balance** imellem behov for dataflow og borgernes rettigheder

Anvendelsesområde

Denne forordning finder anvendelse på **behandling** af **personoplysninger**, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et **register**.

Hvad er behandling?

Enhver aktivitet eller række af aktiviteter som personoplysninger gøres til genstand for

Typer af personoplysninger

Almindelige oplysninger	Personfølsomme oplysninger
Navn, adresse	Race og etnicitet
Mailadresse, telefonnummer	Politisk og **religiøs overbevisning** (dermed er alle persondata i frikirker følsomme – også de almindelige oplysninger i venstre kolonne)
Uddannelse, beskæftigelse ...	Fagforeningsmæssigt tilhørsforhold
Oplysninger om bolig, bil ...	Helbredsoplysninger
Løn, skat og økonomi	Genetiske data
Foto og video	Biometriske data
IP-adresse	Seksuelle forhold og orientering
CPR-nummer (OBS: Dog særlig lov = FORTROLIG)	**Straffedomme / lovovertrædelser (Særlig)**

- **Hvad er personoplysninger?**
  Navn, IP, CPR nr., nr. plade, adresse, familiemæssige oplysninger, kreditkort nr., mailadresse, foto ….

- **Hvad er et register?**
- Dvs. excelark, worddokumenter, e-mails, A4-mapper med lister, databaser, rengskabsprogrammer, webshops, kartotekskort i en kasse …

”Grundloven i GDPR”

- **Persondata skal:**

- Behandles **lovligt**, rimeligt og gennemsigtigt
- Behandles **sagligt** – til udtrykkelige formål (**formålsbegrænsning**)
- Begrænses til, hvad der er **nødvendigt** ift. formål (**dataminimering**)
- Være **korrekte** og ajourførte (**rigtighed**)
- Opbevares så det **ikke** er muligt at identificere de registrerede **længere end nødvendigt** (**opbevaringsbegrænsning**)
- Behandles **sikkert** mod uautoriseret adgang (**integritet og fortrolighed**)

”Hjemmel”

- **Grundregel:**
- Al databehandling skal hvile på et hjemmel

•Der er følgende typer af hjemmel:

- Et **samtykke (personfølsomme data kræver i mange tilfælde samtykke)**
- En **kontraktlig forpligtelse (HR)**
- Et **retslig forpligtelse (Skat)**
- **Beskyttelse** af den registrerede
- En **myndighedsudøvelse**
- **Interesseafvejning** – afvejning af interesse op mod grundlæggende rettigheder
- **Særlige retsregler; Art 9,2,d -** fx må religiøse organisationer mv. gerne gemme personfølsomme oplysninger om deres medlemmer sikkert på deres kontor, men oplysningerne må ikke komme uden for kontoret fx på en adresseliste, hvis der ikke er et udtrykkeligt samtykke fra hver enkelt.
- **Forældresamtykke:** Der skal altid forældresamtykke til ift. opbevaring af persondata på børn under 13 år.

•Ansvar:

- Virksomheden skal kunne påvise og dokumentere, at man overholder dette

Samtykke, som indhentes ved personfølsomme data

- **Skærpede krav til samtykke, som skal være:**
  - Frivilligt
  - Specifikt
  - Informeret
  - Utvetydigt
  - Lige så let at trække tilbage som at give
  - Udtrykkelig
  - Forældresamtykke for børn under 13 år

- **Ansvar:**
  - Kirken skal kunne påvise og dokumentere, at man overholder dette (PP-politik på web)

Medlemmer/støtter/frivillige

- Medlemskab er vedtægtsforankret
  - Jo bredere medlemsdefinition desto flere data at holde styr på (Hvis medlemsdefinition ikke kan adskilles fra tilmelding til nyhedsbrevet, vil man formentlig mene, at tilmelding til nyhedsbrev er personfølsom data)

- Støtter / bidragydere er typisk IKKE vedtægtsforankret, men persondatamæssigt skal de sidestilles

- Frivillige – registrering inden for de enkelte arbejdsområder – fx lovsang, børnekirke, café …

Tænk - Saglighed

- **Grundregel:**
- Al databehandling skal hvile på et sagligt og legitimt formål
- Data skal indsamles til udtrykkelige og gennemsigtige formål ..
  - .. dvs. ikke "måske kunne vi få brug for ....."
- **Data må KUN benyttes til det oplyste og et sagligt formål**

- **Ansvar:**
- Kirken skal kunne påvise og dokumentere, at man overholder dette

Tænk – ”Minimalistisk”

- **Grundregel:**
- Al databehandling skal begrænses til det nødvendige

•**Tre dimensioner af ”minimalistisk”:**

•”Dataminimering”

- ”Hvilke data kan vi nøjes med?”

•Adgangsbegrænsning:

- ”Hvem kan vi nøjes med har adgang?”

•Lagringsbegrænsning

- ”Hvor længe kan vi nøjes med at opbevare data, inden de skal slettes igen?”
- **ALLE persondata har en udløbsdato** – og den skal du vurdere ud fra saglighed og lovgivning

•**Ansvar:**

- Kirken skal kunne påvise og dokumentere, at man overholder dette

Datasubjektets rettigheder

- Virksomheder har en **proaktiv orienteringspligt** ift. alt, hvad man gør med persondata
- Man har ret til **indsigt**
- Man har ret til at få **rettet** forkerte oplysninger
- Man har ret til at blive **slettet og evt. glemt**
- Man har ret til **dataportabilitet –** om muligt
- Man har ret til ikke at blive udsat for ”afgørelser” via **profilering**
- Man har ret til indsigelse mod **direkte markedsføring**

Oplysningspligt - indsamling hos den registrerede selv

Følgende oplysninger skal gives på indsamlingstidspunktet – henvis til privatlivspolitik på hjemmeside (se også næste slide)

- Identitet/kontaktoplysninger på dataansvarlig i forening
- Formål(ene) med behandlingen og retsgrundlaget
- Modtagere eller kategorier af modtagere *fx myndigheder, samarbejdspartnere etc.*
- Om oplysningerne overføres til tredjelande/en international organisation + retsgrundlaget herfor
- Hvor længe oplysningerne behandles eller kriterier til fastlæggelse heraf
- Den registreredes rettigheder
- Retten til at tilbagekalde samtykke
- Retten til at klage til tilsynsmyndigheden
- Hvorvidt det er et lovkrav eller et krav baseret på en kontrakt, at den registrerede afgiver personoplysninger
- Forekomsten af automatiserede afgørelser, herunder profilering, samt opbygning og betydningen heraf

- *Det anbefales at underretningen er skriftlig*
- *Den dataansvarlige er forpligtet til at give meddelelse én gang*
- *Hvis der skal ske viderebehandling til et andet formål, så "ny" oplysningspligt*

Oplysningspligt

Henvis til jeres privatlivspolitik på alt materiale, der har med databehandling at gøre

Sørg for ved den første digitale kontakt at lave LINK direkte til privatlivspolitik på web

Henvis på kontaktkort, medlemslister, arbejdsgruppeliste mv.

Den må IKKE være svær at finde

Hav jeres vedtægter, medlemsdefinition mv. samme sted, så det er nemt at se, hvad det betyder for MIG – lige NU

Den dataansvarlige har en sletteplig

- Ikke længere nødvendigt at behandle oplysningerne
- Samtykke trækkes tilbage, og der er ikke et andet behandlingsgrundlag
- Begrundet indsigelse mod behandling i medfør af Art 6, stk. 1, litra (e) eller (f)
- Indsigelse mod behandling til direkte markedsføring + profilering i dette øjemed
- Ulovlig behandling af personoplysninger
- Følger af national ret eller EU-ret
- Vedrører behandling af oplysninger baseret på samtykke fra barn Ovenstående gælder ikke, såfremt: 1) informations/ytringsfrihed, 2) retlig forpligtelse/opgave i samfundets interesse, 3) folkesundhed, 4) arkivformål mv. 5) nødvendig for at et retskrav kan fastlægges, gøres gældende eller forsvares.

  OBS: den dataansvarlige skal i rimeligt omfang foranstalte sletning i videre led, jf. Art 17, stk. 2 Ret til sletning - "retten til at blive glemt"

- Den registreredes ret til at få sine oplysninger ”med sig” hvis:
  - behandlingen er baseret på samtykke eller kontraktopfyldelse, og
  - behandlingen foretages automatisk

- Retten til dataportabilitet omfatter kun oplysninger, som den registrerede ”selv” har givet til den dataansvarlige

- Hvis teknisk muligt, så omfatter retten til dataportabilitet en ret til at få oplysningerne ”transmitteret” direkte fra den dataansvarlige til en anden

Fortegnelse over behandlingsaktiviteter

- **Er et krav – hvis:**
- Virksomheden har over 250 medarbejdere eller
- Virksomheden behandler personfølsomme data (og dermed for alle frikirker) eller
- Virksomheden behandler persondata lejlighedsvis eller
- Virksomhedens aktiviteter sandsynligvis vil medføre en risiko for de registrerede

Omfatter en **registrering pr. behandlingsaktivitet af** (skabeloner til disse udsendes):

- Navn og kontaktoplysninger på den dataansvarlige
- Formål med behandling
- Kategorier af registrerede og kategorier af personoplysninger
- Kategorier af modtagere af personoplysninger
- Om muligt – forventede tidsfrister for sletning
- Om muligt – beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger

Håndtering af databrud …

- **Orientering af Datatilsynet:**
- ”Uden ugrundet ophold"
- Ikke senere end 72 timer efter, at man har opdaget dette
  - Hvad er der sket
  - Konsekvenser
  - Foranstaltninger, der er truffet for at håndtere bruddet og mindske skadevirkninger

- **Orientering af datasubjekterne:**
- Hvis der er en høj risiko for misbrug af data

Det er nødvendigt …

- … at have styr på den traditionelle IT-sikkerhed.

- At der er styr på jura betyder jo ikke, at man ikke kan komme til at lække data.

- Betyder **fokus på:**
- Opdaterede virussystemer
- Programmer, som er sikkerhedsmæssigt opdateret
- Login procedurer
- Firewalls
- Backup
- …

Holdninger og især adfærd
er årsagen til 8-9 ud af 10 datalæk

Sætter stort fokus på adfærd i forhold til:

- Mails med vedhæftede links og filer
- Besøgte hjemmesider
- Installation af eksterne programmer

Hvordan tænker jeg om persondata og sikkerhed

Tal og bogstaver, jeg skal bruge i mit arbejde.

Sat sammen i CPR-nr., mail-adresser mv.

En delmængde af personlig integritet, som kunder / kolleger har betroet min virksomhed (og dermed mig) i min varetægt

Sikkerhedsniveau afhænger af adfærd/sund fornuft

- **Hvordan omgås jeg persondata – herunder lagring og videresendelse:**
  - Adgangsrettigheder
  - Brug af secure mails – ift. eksterne
  - Hvor lægger man datafiler henne
  - Sender man dokumenter med persondata rundt og ud af huset på ikke-sikre forbindelser
  - Hvordan er adfærden ift. printet materiale med persondata
  - Taler man så højt og på steder, at andre kan opfatte vitale persondata

- **Behandler jeg passwords som undertøj:**
  - Skift det – del det ikke – vær mystisk – lad det ikke ligge og flyde

- **Praktisk adfærd ift. brug af IT-udstyr:**
  - Luk altid skærmen, når den forlades
  - Luk bærbare PC inde om natten

Hvornår sletter vi data?

- **Generelle regler:**
  - 5 år + indeværende = bogføringsloven
    gælder også for HR dvs. ansættelseskontrakter, løn mv.
  - 3 år = Skat
    - Gaveskema – 03.012 / 03.013
  - Noget sletter vi NU – husk indbakken
  - Brug sikker mail ved personfølsomme data

LAV KLARE SLETTEPOLITIKKER og procedurer for sikring af overholdelse

De 12 spørgsmål

1. Har organisationen kendskab til den nye databeskyttelsesforordning?
2. Hvilke personoplysninger behandler I?
3. Hvilken information giver I de registrerede?
4. Hvordan opfylder I de registreredes rettigheder?
5. På hvilket grundlag behandler I personoplysninger?
6. Hvordan indhenter I samtykke?
7. Behandler I personoplysninger om børn?
8. Hvad skal I gøre ved brud på datasikkerheden?
9. Er jeres behandlinger forbundet med særlige risici?
10. Har I indtænkt databeskyttelse i jeres systemer?
11. Hvem er ansvarlig for databeskyttelsesspørgsmål i organisationen?
12. Driver I virksomhed i flere lande?