Persondata forordning i praksis

VED VESTJYSK EDB CENTER

Vestjysk EDB Center

Foredrags holderen:

Christian Christensen

Ejer af Vestjysk EDB Center Aps siden 1992

Bygger og monterer IT løsninger for virksomheder og private.

Har gennem årene fulgt udviklingen gennem en lang række kurser og certificeringer.

Arbejder primært med infrastruktur og tilpasninger. Supporterer og administrerer virksomhedsløsninger og standard programmer incl. regnskabs programmer.

Som frivillig:

formand for Borgerforeningen I Vorgod-Barde

Medlem af Landdistriktsrådet

Vestjysk EDB Center

Udfordring - kulturændringer?

Det kan kræve en kulturændring

– er du klar til det?

Vaner og procedurer skal ændres.

Ledere skal forstå og anerkende

Papirarbejdet skal klares.

Ordbogen:

GDPR = General Data Protection Regulation => Persondataforordningen

Datasubjekt = kunden/borger/medlem

Den dataansvarlige = den, der indsamler data til specifik formål (altid dig selv)

Databehandler = den, der på dine vegne håndterer og har adgang til dine data

- Underdatabehandler = 3. parter, der er knyttet til databehandler.

Persondata = alle data, der kan knyttes direkte eller indirekte til en person. Små virksomheder og personejede virksomheder er også persondata.

DPIA = Data Protection Impact Assessment = kortlægning af databeskyttelse = særlige tilfælde

DPO = Data Protection Officer = er til større virksomheder – ofte offentlige, næsten ingen skal bruge det i Danmark. Til virksomheder med mere end 250 medarbejdere.

Hvad er persondata?

Kategori	Persondataloven	Persondataforordningen
Almindelige oplysninger	• Navn • Adresse • Telefonnummer • Fødselsdato • Uddannelse • Beskæftigelse • Eksamensresultater • Bolig og bil • Løn og skat • Sygefravær m.v.	Omfatter herudover: • Væsentlige sociale problemer • Andre rent private forhold end følsomme oplysninger • CPR-nr. Særlig kategori • Oplysninger om strafbare forhold
Semi-følsomme oplysninger	• Oplysninger om strafbare forhold • Væsentlige sociale problemer • Andre rent private forhold end følsomme oplysninger	
Følsomme oplysninger	• Race • Etnisk oprindelse • Politisk religiøs eller filosofisk overbevisning • Fagforeningsmæssigt tilhørsforhold • Seksuelle forhold og seksuel orientering • Helbredsoplysninger	Omfatter herudover: Genetiske og biometriske data

Anonyme oplysninger

Pseudonyme oplysninger ✓

Hvad er personoplysninger?

Cpr-nr.

Køn

Navn

Race

Adresse

E-mail-adresse

Seksuel overbevisning

Foto

Fødselsdato

Kreditkortnummer

Adgangskontrol

Helbredsoplysninger

Nummerplade

Genetisk information

Interesser

Familiemæssige oplysninger

MedarbejderID

Politisk overbevisning

Væsentlige sociale problemer

Uddannelse (karakterer)

Personlighedstest

Telefonnummer

Religion

Personlige produktionstal

IP-adresse

Elektroniske spor

Videoovervågning

Pasnr.

GPS-oplysninger

Logning i IT-systemer

Initialer/Loginnavn

Fagforeningsmæssige tilhørsforhold

Biometriske oplysninger

Straffeattest

Stilling

Størrelse på tøj og sko

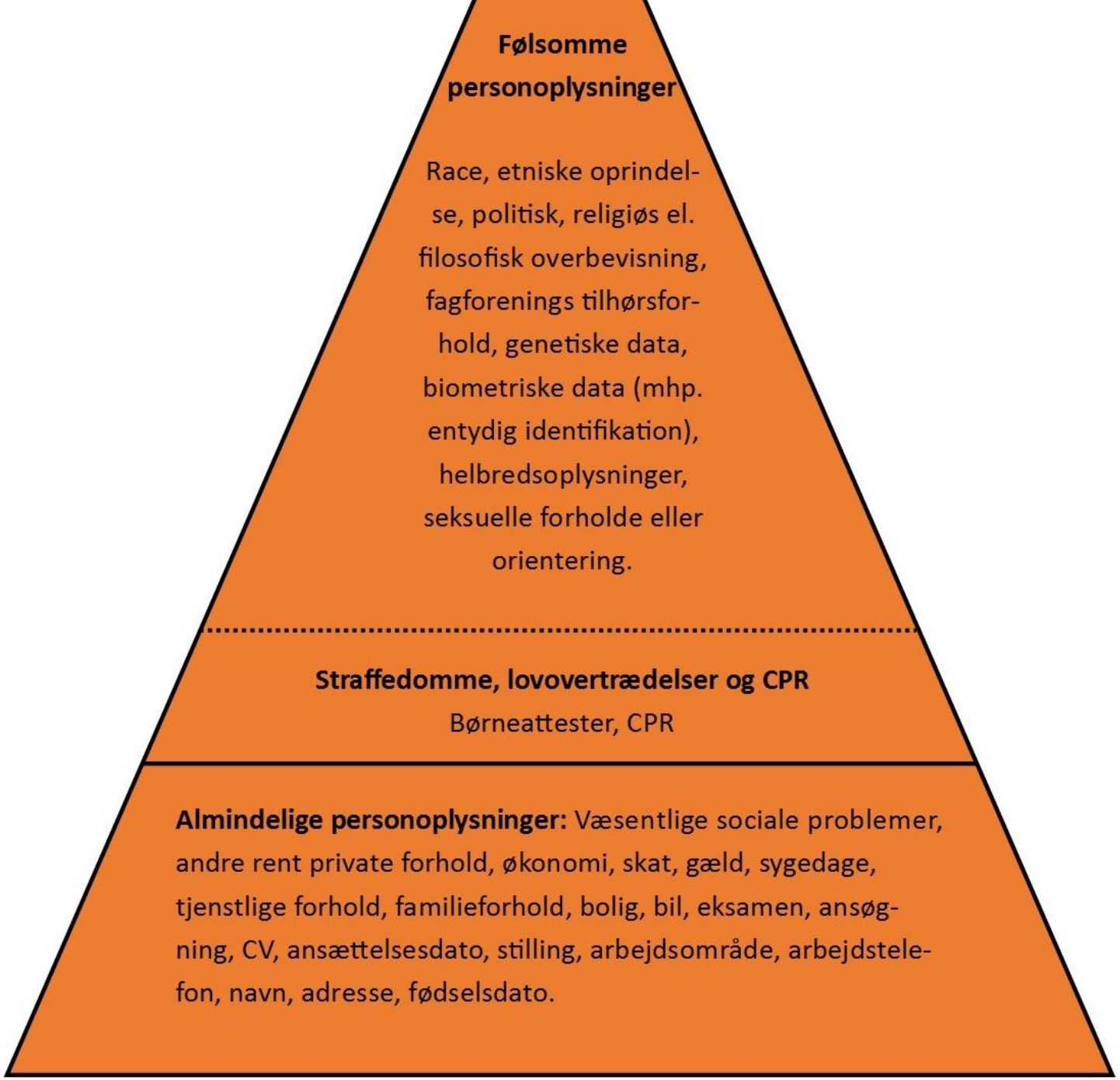
Rejseoplysninger

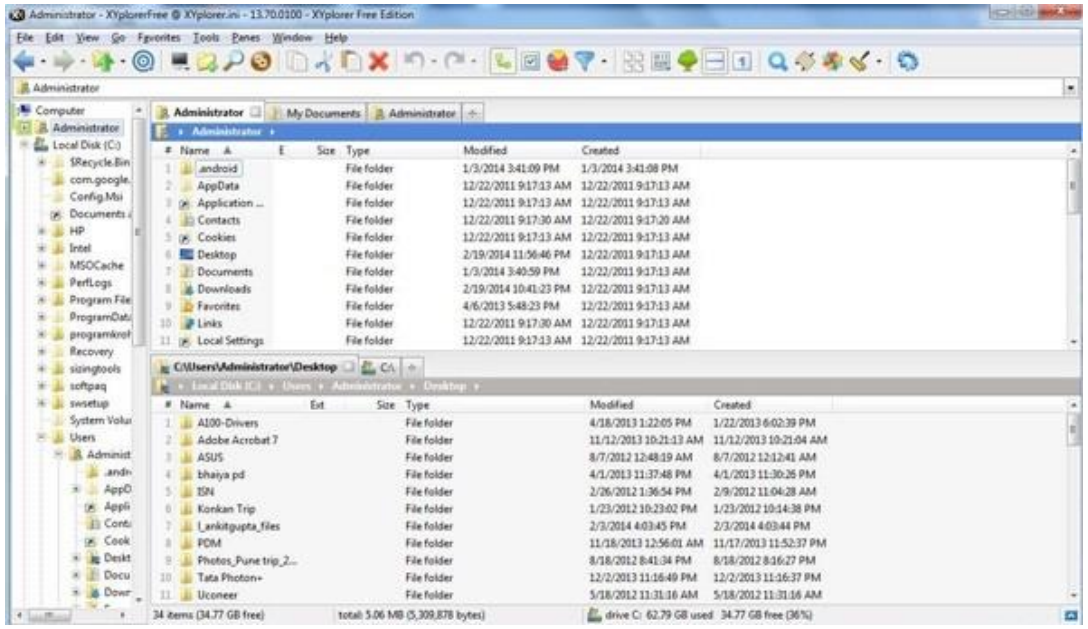
MAC-adresse

Løn

De tre kategorier af personoplysninger:

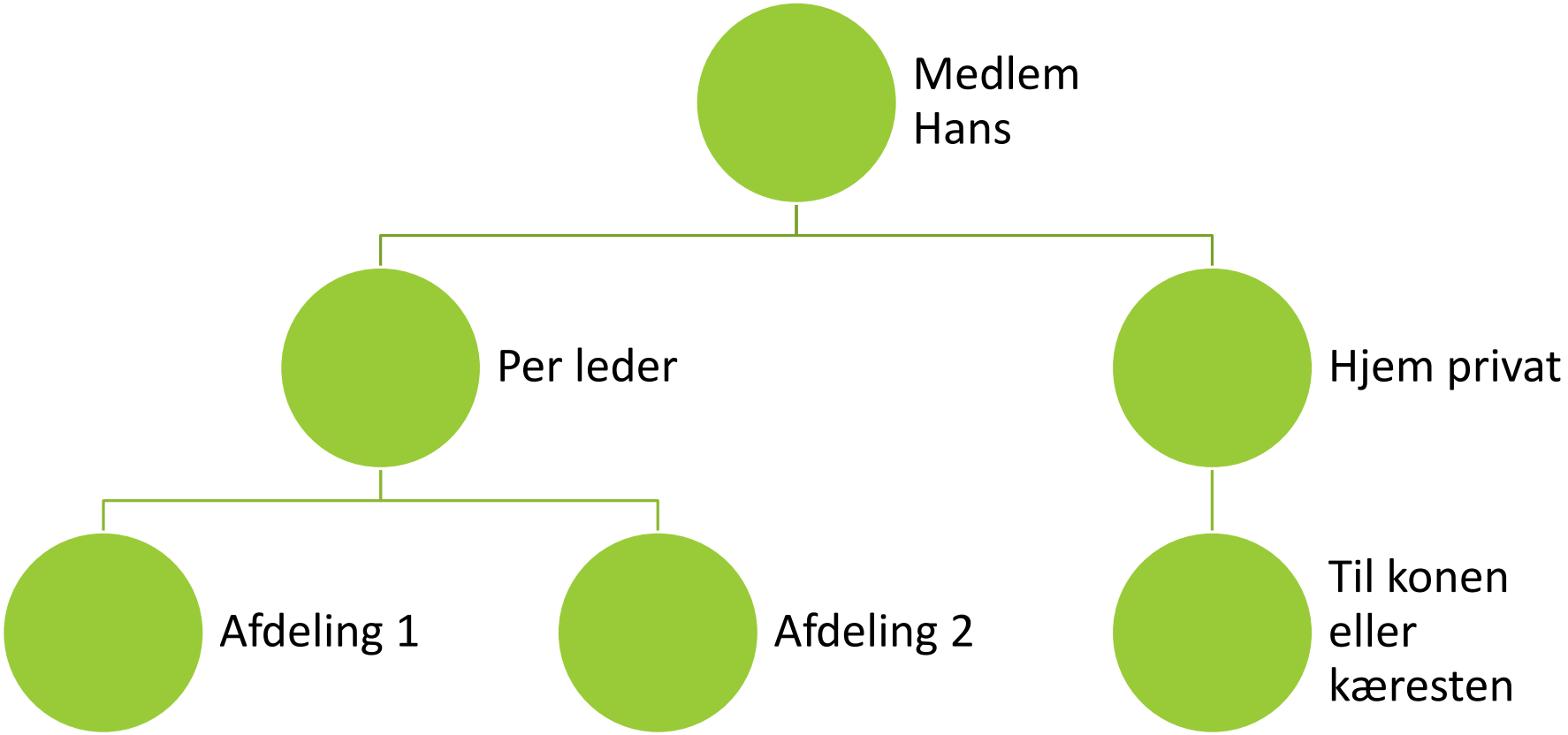
Jo højere oppe i trekanten oplysningerne er, desto strengere er betingelserne for at I må behandle dem.





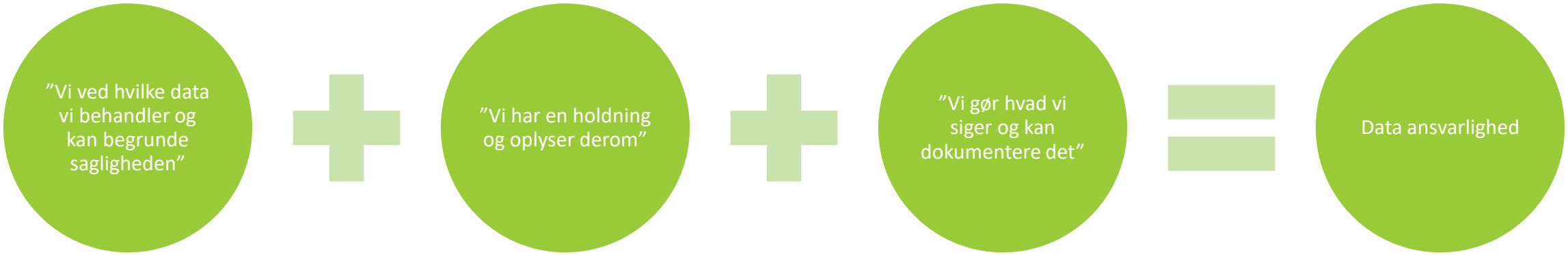
Hvor er data og hvem har dem ?

Hvor er mailen?



Hvem har ansvaret?

Den dataansvarlige skal indføre foranstaltninger for at sikre og være i stand til at dokumentere overholdelse af forordningen.



Principper for behandling af data

Vigtig slide

En af de mest centrale artikler. Forstå den = giver en god ide om hvad hele persondataforordningen går ud på

Forordningens artikel 5

- Lovligt, rimeligt og gennemsigtigt (”saglighed”)
- Indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål (”formålsbestemthed”)
- Være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvor de behandles (”dataminimering”)
- Være rigtige og om nødvendigt ajourførte (”rigtighed”)
- Opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt (”lagringsbegrænsning”)
- Behandles på en måde, der sikrer tilstrækkelig sikkerhed (”integritet og fortrolighed”)

Den dataansvarlige forpligtigelse

Dokumentation?

- Den dataansvarlige skal kunne dokumentere compliance med forordningen (Artikel 30 fortegnelsen)
- Både dataansvarlige (og databehandlere) skal opbevare dokumentation for enhver behandling af personoplysninger
- Dokumentationen skal mindst omfatte (privatlivs politik):
  - Navn og kontaktoplysninger på den dataansvarlige eller den fælles dataansvarlige og dennes eventuelle repræsentant
  - Formålene med behandlingen
  - Beskrivelse af kategorier af registrerede og kategorier af personoplysninger
  - Kategorier af modtagere af personoplysningerne
  - En generel angivelse af tidsfristerne for sletning af de forskellige kategorier af personoplysninger
  - Hvis muligt, en beskrivelse de tekniske og organisatoriske sikkerhedsforanstaltninger

Rettigheder og pligter.

Foreningers **registrering** af oplysninger om medlemmerne er omfattet af databeskyttelsesretten. Det er Datatilsynets opfattelse, at en forening kan registrere almindelige oplysninger som f.eks. indmeldelsesdato, id-oplysninger, evt. tillids- eller hvervsposter m.m. En forening vil som udgangspunkt også kunne registrere oplysninger af mere speciel karakter som f.eks. oplysninger om et medlems bedste score, golfhandicap, certifikat niveau m.m.

Ved **videregivelse** af medlemsoplysninger skal der ifølge Datatilsynets praksis skelnes mellem to situationer:

Videregivelse af medlemslister i foreningsblade m.v**.** kan som udgangspunkt ske uden den enkeltes (medlemmets) samtykke under forudsætning af, at bladet kun distribueres til medlemmer.

Derimod kræver videregivelse i form af offentliggørelse på internettet det enkelte medlems samtykke. Datatilsynet er af den opfattelse, at medlemskab af en forening, uanset at denne måtte være en ukontroversiel - f.eks. en sportsforening, er en privat sag. Tilsynet lægger også vægt på, at der vil være en risiko for, at medlemsoplysningerne vil blive (mis-)brugt til uvedkommende formål, f.eks. markedsføring. Offentliggørelse af en oplysning om en persons medlemskab kræver derfor det enkelte medlems samtykke.

Datatilsynet ligestiller i sin praksis lukkede sider på internettet med et foreningsblad m.v. under forudsætning af, at det f.eks. ved hjælp af password eller lignende sikres, at kun medlemmer har adgang til den pågældende side.

Samtykke

Datatilsynets definition

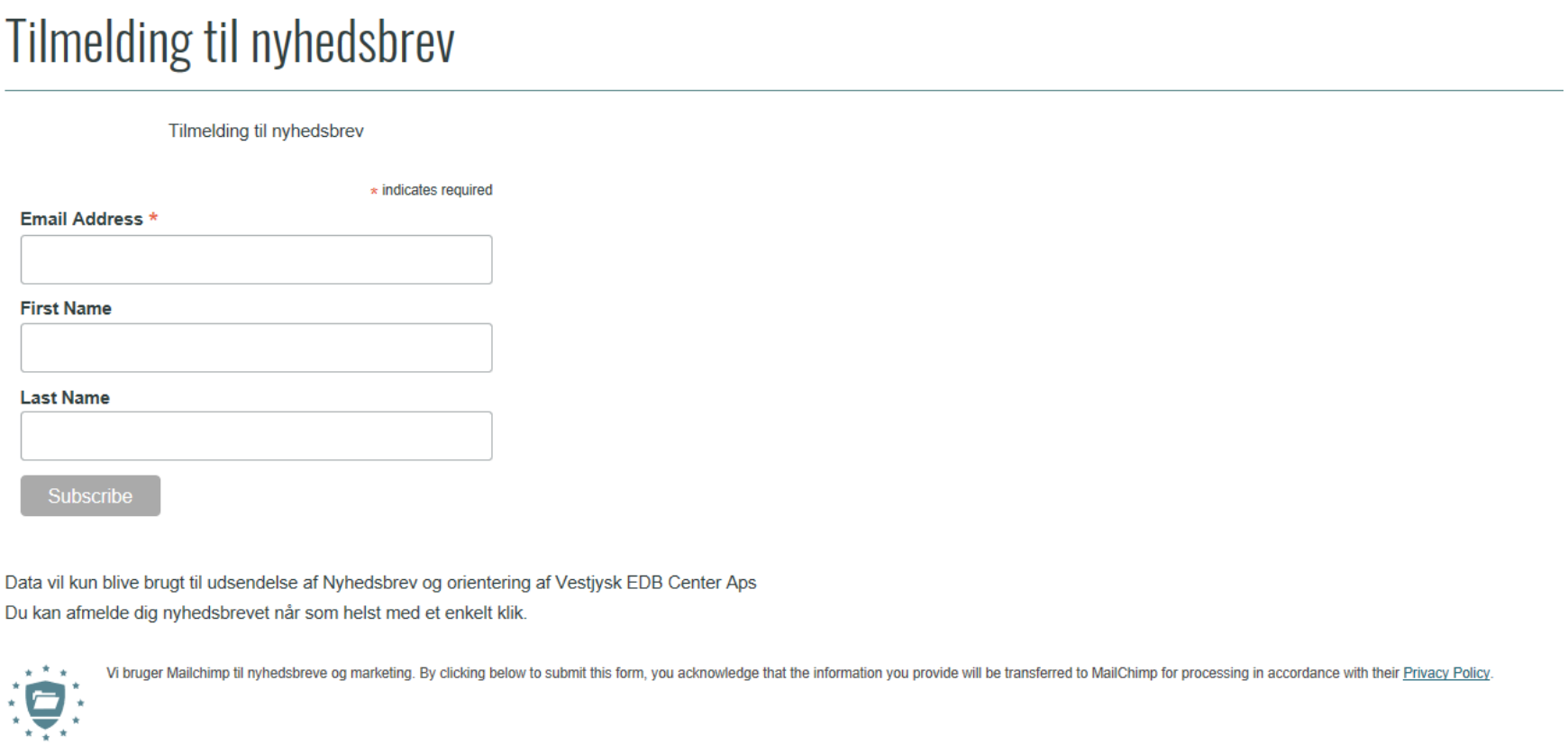
”Enhver, frivillig, specifik, informeret og utvetydig viljestilkendegivelse, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling.”

Det er endvidere et krav, at den dataansvarlige kan påvise, at den registrerede har givet samtykke til behandlingen af sine personoplysninger. Det er med andre ord den dataansvarlige, som har bevisbyrden for, at den registrerede har givet det fornødne samtykke.

Herudover gælder, at hvis den registreredes samtykke gives i en skriftlig erklæring, der også vedrører andre forhold, skal en anmodning om samtykke forelægges på en måde, som klart kan skelnes fra de andre forhold, i en letforståelig og lettilgængelig form og i et klart og enkelt sprog.

Endelig er det et krav, at den registrerede, inden samtykke gives, skal oplyses om, at samtykket kan trækkes tilbage.

Eksempel



Tilmelding til nyhedsbrev

Tilmelding til nyhedsbrev

* indicates required

Email Address *

First Name

Last Name

Subscribe

Data vil kun blive brugt til udsendelse af Nyhedsbrev og orientering af Vestjysk EDB Center Aps
Du kan afmelde dig nyhedsbrevet når som helst med et enkelt klik.

Vi bruger Mailchimp til nyhedsbreve og marketing. By clicking below to submit this form, you acknowledge that the information you provide will be transferred to MailChimp for processing in accordance with their Privacy Policy.

Vestjysk EDB Center

Eksempel fra hjemmeside

Personoplysninger

Generelt
Personoplysninger er alle slags informationer, der i et eller andet omfang kan henføres til dig. Når du benytter vores website indsamler og behandler vi en række sådanne informationer. Det sker f.eks. ved alm. tilgang af indhold, hvis du tilmelder dig vores nyhedsbrev, deltager i konkurrencer eller undersøgelser, registrerer dig som bruger eller abonnent, øvrig brug af services.

Vi indsamler og behandler typisk følgende typer af oplysninger: Et unikt ID og tekniske oplysninger om din computer, tablet eller mobiltelefon, dit IP-nummer, geografisk placering, samt hvilke sider du klikker på (interesser). I det omfang du selv giver eksplicit samtykke hertil og selv indtaster informationerne behandles desuden: Navn, telefonnummer, e-mail, adresse og betalingsoplysninger. Det vil typisk være i forbindelse med oprettelse af login eller ved køb.

Desuden viser vi medlemsnummer og navn på hjemmesiden (dette kan fraviges efter ønske).

Sikkerhed
Vi har truffet tekniske og organisatoriske foranstaltninger mod, at dine oplysninger hændeligt eller ulovligt bliver slettet, offentliggjort, fortabt, forringet eller kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med lovgivningen.

Formål
Oplysningerne bruges til at identificere dig som bruger og vise dig de annoncer, som vil have størst sandsynlighed for at være relevante for dig, at registrere dine køb og betalinger, samt at kunne levere de services, du har efterspurgt, som f.eks. at fremsende et nyhedsbrev. Herudover anvender vi oplysningerne til at optimere vores services og indhold.

Periode for opbevaring
Oplysningerne opbevares i det tidsrum, der er tilladt i henhold til lovgivningen, og vi sletter dem, når de ikke længere er nødvendige. Perioden afhænger af karakteren af oplysningen og baggrunden for opbevaring. Det er derfor ikke muligt at angive en generel tidsramme for, hvornår informationer slettes.

Videregivelse af oplysninger
Vi benytter en række tredjeparter til opbevaring og behandling af data. Disse behandler udelukkende oplysninger på vores vegne og må ikke anvende dem til egne formål.

Videregivelse af personoplysninger som navn og e-mail m.v. vil kun ske, hvis du giver samtykke til det. Vi anvender kun databehandlere i EU eller i lande, der kan give dine oplysninger en tilstrækkelig beskyttelse.

3. parts databehandler:

- www.conventus.dk, dine kontaktinformationer og tilknytninger bliver gemt i 36 måneder

Indsigt og klager
Du har ret til at få oplyst, hvilke personoplysninger, vi behandler om dig. Du kan desuden til enhver tid gøre indsigelse mod, at oplysninger anvendes. Du kan også tilbagekalde dit samtykke til, at der bliver behandlet oplysninger om dig. Hvis de oplysninger, der behandles om dig, er forkerte har du ret til at de bliver rettet eller slettet. Henvendelse herom kan ske til: formand@vorgod-barde.dk. Hvis du vil klage over vores behandling af dine personoplysninger, har du også mulighed for at tage kontakt til Datatilsynet.

Udgiver
Websitet ejes og publiceres af:

Vorgod-Barde Borgerforening

Kongevejen 15, 6920 Videbæk

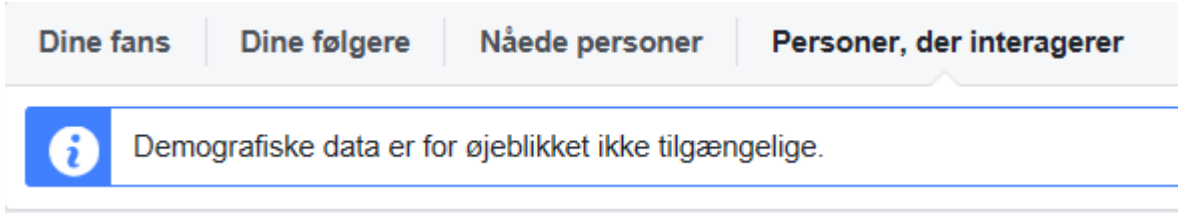
mail: formand@vorgod-barde.dk

Almindelige oplysninger

Det er Datatilsynets opfattelse, at en forening kan registrere almindelige oplysninger som f.eks. indmeldelsesdato, id-oplysninger, evt. tillids- eller hvervsposter m.m. En forening vil som udgangspunkt også kunne registrere oplysninger af mere speciel karakter som f.eks. oplysninger om et medlems bedste score, golfhandicap, certifikat niveau m.m.

NYT

Fælles Dataansvar



Konklusionen i Datatilsynets vurdering på ny EU dom lyder:

EU-Domstolen har den 5. juni 2018 afsagt en dom om bl.a. dataansvaret for såkaldte fansider på Facebook (også kaldet Facebook-sider - ikke at forveksle med privatpersoners Facebook-profiler).

Dommen fastslår bl.a., at Facebook og administratoren af en fanside har et fælles dataansvar for behandlingen af personoplysninger, som bliver indsamlet i forbindelse med besøg på den pågældende fanside.

Datatilsynet har læst dommen grundigt igennem og giver nu sin vurdering af, hvad dommen i en dansk kontekst betyder for administratorer af fansider på Facebook, og hvad de bør være opmærksomme på for at leve op til databeskyttelseslovgivningen.

Datatilsynet vil arbejde for, at Facebook medvirker til en løsning.

Eksempel: https://www.facebook.com/vorgodbarde

Minimumindhold af databehandleraftale

- En beskrivelse af emnet, varigheden, arten og formålet med behandlingen, typen af data, kategorier af datasubjekter samt den dataansvarliges forpligtelser og rettigheder
- Instruktionsbeføjelse
- Krav om fortrolighed hos autoriserede personer
- Betingelse om, at der kun må bruges underdatabehandlere med den dataansvarliges
- forudgående skriftlige samtykke
- Betingelse om at databehandleren bistår med at besvare henvendelser fra datasubjekter
- Krav om implementering af sikkerhedskrav
- Betingelse om at databehandleren bistår med overholdelse af forpligtelserne ift. personoplysningssikkerhed:
  - Behandlingssikkerhed
  - Anmeldelse af sikkerhedsbrud til myndighed og eventuelt datasubjekter
  - Konsekvensanalyse og forudgående høring
- Betingelse om, at persondata skal slettes eller returneres ved aftalens ophør
- Betingelse om, at databehandler dokumenterer overholdelse af aftalen og tilladelser.

Vestjysk EDB Center

Privacy by default

Persondatabeskyttelse skal være udgangspunktet!

- Privatlivsfremmende indstillinger skal være slået til som standard
- Eksempel:
  - Du opretter dig på et socialt medie, og standard indstilling er, at den viser dit navn, adresse, lokation og venneforbindelser.
  - Der er en indstilling, som skjuler din adresse, lokation og venne forbindelser.
  - Privacy by default betyder, at denne indstilling skulle været slået til fra start.
- Privacy by default gælder også
  - Nyhedsbrev tilmeldinger
  - Mobil apps-adgang til persondata som lokation, kontakter, osv.
  - Adgangsstyring til jeres egne persondata
  - F. eks.: bruger medarbejder eget udstyr eller forening/erhverv. Blandes privat og forening/erhverv?

Privacy by design[1:2]

Tænk sikkerhed ind i koden, design og valg af systemer (spørg leverandør og stil krav)

Alle teknologier, produkter og services, der behandler persondata, skal designes med persondatasikkerhed og overholdelse af forordningen in mente.

Privatlivsfremmende teknologier

- Kryptering–beskyt data 'at rest' med kryptering, ex. filer eller databasefelter
- Adgangsbegrænsning ift. Data - Hvilke personer bør have adgang til hvilke data? (skal tages udgangspunkt i datasubjektets sikkerhed)
- Log management – sørg for registrering af, hvem der har tilgået hvilke data og hvornår (informer)
- Data LossPrevention – teknisk kontrol af om persondata forlader foreningen.

…fortsættes

Privacy by design[2:2]

- Privatlivsfremmende teknologier

- Anonymisering–data er ikke længere persondata, men i praksis svær…
  - Må aldrig nogensinde kunne kædes tilbage til en person
  - Fx summér resultater i en spørgeskemaundersøgelse, og smid de individuelle svar væk.
- Pseudonymisering–fjern personen fra data
  - Stadig persondata, men høj grad af beskyttelse
  - Ét datasæt indeholder de følsomme oplysninger, ét datasæt indeholder personerne, ét datasæt indeholder referencen mellem 'følsomme oplysninger' og 'personer'
  - Kun ved at have alle 3 datasæt kan data bruges til noget.

Indsigtsretten

Den dataansvarlige skal efter anmodning fra datasubjektet give datasubjektet indsigt i:

- Om den dataansvarlige behandler personoplysninger om datasubjektet
- Adgang til personoplysningerne
- Følgende informationer:
  - Formålene med behandlingen
  - Kategorierne af personoplysninger
  - Kategorier af modtagere
  - Opbevaringstid (eller hvordan denne beregnes)
  - Oplysninger om rettigheder
  - Retten til at klage til myndigheder
  - Oplysning om, hvor personoplysningerne stammer fra
  - Oplysning om brugen af automatiske afgørelser, herunder profilering
  - De fornødne garantier, hvis overførsel til tredjeland

Indsigtsretten –praktisk vinkel

- Automatiseret persondataudtræk – udarbejd en eksportmulighed, hvor medlemmet selv kan se, hvad der er registreret af persondata omkring dem og gemme det i pdf-format (svært!).
- Slettefunktion–hvis et datasubjekt tilbagekalder deres samtykke til behandling af data, skal der indbygges en slettefunktion af kundens data, såfremt tilbagekaldelsen er berettiget.
- Husk ved recovery funktioner at få slettet data igen. Backup data på bånd og diske er også relevante at tage hensyn til.

Vestjysk EDB Center

Retten til at blive glemt

Den dataansvarlige skal slette data uden ugrundet ophold, hvis:

- Formålet er opfyldt
- Samtykke tilbagekaldes, og der er ikke er anden hjemmel
- Datasubjektet gør indsigelse, og den dataansvarlige har ikke tungere vejende grunde til behandling
- Datasubjektet gør indsigelse mod, at den dataansvarlige behandler data med henblik på direkte markedsføring
- Behandlingen er ulovlig.

Undtagelser

Ytringsfrihed, retligt krav, bogføringsloven, garanti aftaler etc.

Hvad skal du gøre nu?

✓ Spørgsmål til besvarelse

1. Har jeres organisation kendskab til den nye databeskyttelsesforordning?
2. Er informationerne, som I ønsker at behandle, omfattet af forordningen; er informationerne at betragte som personoplysninger?
3. Hvilken information giver I de registrerede?
4. Hvordan opfylder I de registreredes rettigheder?
5. På hvilket retligt grundlag behandler I personoplysninger?
6. Hvordan indhenter I samtykke?
7. Behandler I personoplysninger om børn?
8. Hvad skal I gøre ved brud på persondatasikkerheden?
9. Er jeres behandlinger forbundet med særlige risici
10. Har I indtænkt databeskyttelse i jeres it-systemer?
11. Hvem er ansvarlig for databeskyttelsesspørgsmål i jeres organisation?

Her sætter du et "flueben", når spørgsmålet er besvaret

Vestjysk EDB Center

Her følger vores tre råd om, hvordan I kommer i gang:

Få overblik og information. Start med at læse Datatilsynets Generel informationspjece om Databeskyttelsesforordningen. Pjecen er nem at læse, giver overblik over loven og beskriver reglerne på en lettilgængelig måde.

Skab overblik over, hvilke data I opbevarer. Det kan fx være medlems- eller brugeroplysninger som navn, adresse, mail og personnummer. Derefter skal I lave en liste med de leverandører, der opbevarer data for jer - eller som I deler data med. Det kan være en ekstern revisor eller virksomheder, der leverer IT-programmer som fx en medlemsdatabase eller et bookingsystem. I skal indgå en databehandleraftale (se næste punkt) med alle disse leverandører.

Fortegnelse, privatlivspolitik og databehandleraftaler.

- **Fortegnelse.** I skal lave en såkaldt fortegnelse, der beskriver, hvordan I behandler de data, I opbevarer, og hvorfor I opbevarer data som fx medlemsoplysninger. Det er et krav, at fortegnelsen er skrevet ned. Datatilsynet har udgivet Vejledning om fortegnelse, som giver en udførlig beskrivelse af, hvordan I udformer en fortegnelse.
- **Privatlivspolitik.** Dokumentet skal beskrive over for jeres medlemmer og brugere, hvordan I behandler personoplysninger, hvorfor I opbevarer bestemte oplysninger (f.eks telefonnummer), og hvem medlemmer/brugere kan henvende sig til, hvis de vil have slettet deres data.
- **Databehandleraftale.** I skal indgå en databehandleraftale med samarbejdspartnere og leverandører, der opbevarer data for jer. Datatilsynet har udarbejdet en skabelon til en databehandleraftale, men mange professionelle samarbejdspartnere som fx revisionsfirmaer har også skabeloner, I kan tage udgangspunkt i. Vær særligt opmærksomme på, om I bruger cloud-løsninger som Dropbox og Google Drev til at opbevare fx medlemsoplysninger. Cloud-leverandører anvender ofte standardvilkår, som ikke nødvendigvis overholder EU's persondataforordning. Kontakt Datatilsynet, hvis I er i tvivl.

Forpligtelse ved brud

Orienteringsforpligtelse for den dataansvarlige

72 timers deadline for at orientere Datatilsynet

Uden ugrundet ophold skal der redegøres for:

- Sikkerhedsbruddets karakter
- Konsekvenser af sikkerhedsbruddet, herunder omfang af berørte personer m.v.

Vigtigt med dokumentation af alle relevante forhold omkring sikkerhedsbruddet.

Konklusion: Hvis databehandler opdager eller bliver orienteret om et sikkerhedsbrud, så bør de give jer et overblik og underrette den dataansvarlige inden for 48 timer.

OBS: Omvendt bevisbyrde!

Datatilsynets behandling af brud ☺

Den primære sanktion bliver

- vejledning
- påtaler
- grove irettesættelser
- Påbud
- Evt. bøder

når man overtræder databeskyttelsesreglerne.

Kilder til mere information

- Officiel lovtekst(dansk og engelsk)
- Datatilsynet –databeskyttelsesreformen
- DGI persondata side
- Frivillighed.dk
- GDPR mobile app(iTunes)

Tak for denne gang

Vestjysk EDB Center

KONGEVEJEN 15, 6920 VIDEBÆK

TLF. 70202116, MAIL INFO@VESTJYSK-EDB.DK