Persondataforordningen kommer – hvad gør man?
- Guide til virksomheder

Hvad er persondataforordningen?

EU har vedtaget en forordning, der opstiller regler for behandling af persondata. Persondata er alle de data, der kan identificere mennesker, typisk enten jeres kunder eller jeres medarbejdere. Hensynet bag forordningen er at beskytte fysiske personer mod forkert og unødvendig registrering.

Længere nede er angivet eksempler på, hvad persondata er.
Forordningen regler bliver suppleret af danske regler, som fastsættes i Databeskyttelsesloven. **Forordningen og Databekyttelsesloven træder i kraft den 25. maj 2018.**

Hovedprincipperne i forordningen er generelt de samme, som i den gældende lov. Hovedprincipperne er følgende:

LEGITIMITET/SAGLIGHED: Persondata skal være indsamlet til udtrykkeligt angivne formål og må ikke behandles i strid med dette/disse formå

LOVLIGHED: Persondata skal være behandles med hjemmel i en af de hjemler, der er nævnt i forordningen art. 6, f.eks. på baggrund af en kontrakt (ex.vis ansættelseskontrakt), efter samtykke mv.

DATAMINIMERING: Persondata skal være relevante og må ikke omfatte mere end nødvendigt.

RIGTIGHED: Persondata skal være korrekte og ajourførte. Der indføres en ret for den registrerede til at få adgang til at gøre indsigelse samt få rettet sine oplysninger.

OPBEVARING: Persondata må kun opbevares, så længe de er nødvendige, dvs. krav om sletning. Der indføres en ret for den registrerede til at blive glemt.

GENNEMSIGTIGHED: Den registrerede skal oplyses om data og formål mv. og får adgang til indsigt i egne personoplysninger.

DOKUMENTATION: Virksomhederne skal have langt mere styr på og overblik over sine dataprocesser.

BØDER: Der indføres markant større bødeniveau på op til 4 % af omsætningen (på niveau med konkurrencesager).

Hvad er persondata?

Alle oplysninger om *fysiske personer*, som kan identificere vedkommende (både direkte og indirekte).

Eksempler: Navn, cpr.nr., telefonnummer, foto, helbredsoplysninger, referencer, strafbare forhold, religion m.m.

Anonyme oplysninger er ikke omfattet.

Oplysninger om *kapitalselskaber* (dvs. A/S og ApS) er ikke omfattet.

Personligt drevne virksomheder (dvs. enkeltmandsfirmaer og personlige interessentskaber) er omfattet.

1. Lav en dataanalyse

Skab overblik over følgende:

1. Hvordan behandler I medarbejder- og HR-data?

2. Hvordan behandler I kundedata?

3. Hvordan behandler i eventuelle andre persondata?

Kig især på:

- Hvor overføres dataene til – samarbejdspartnere, tredjelande uden for EU/EØS?
- Hvem har adgang (både fysisk og teknisk) til dataene?
- Hvordan er sikkerheden?
- Hvad gør I, hvis I oplever et brud?
- Hvilke data behandler I (almindelige og følsomme personoplysninger)?

Opdeling af oplysninger efter persondataforordningen:

Almindelige personoplysninger (ikke udtømmende oplistet)	**Følsomme personoplysninger** (udtømmende oplistet)
- Køn - Navn - Adresse og mailadresse - Cpr.nr. (særregler ved videregivelse) - Foto (samtykke kræves ved brug på nettet) - Løn og skat - Sygefravær (ikke helbredsoplysninger dog) - Strafbare forhold (dog i særlig kategori) - Personlige produktions- /salgstal - Interesser - Elektroniske spor	- Race og etnisk oprindelse - Politisk, religiøs eller filosofisk overbevisning - Fagforeningsmæssigt tilhørsforhold - Genetisk og biometrisk data - Helbredsoplysninger - Seksuel overbevisning Begrebet semi-følsomme oplysninger udgår!

Tag allerede nu fat i jeres IT-leverandører (f.eks. leverandører af bookingsystemer, lønbureaer, webmaster mv.) for at få overblikket.

2. Overholder I Datatilsynets 12 minimumskrav?

Forordningen har stor fokus på sikkerhed vedr. behandlingen af persondata. Derfor er det vigtigt, at man sikere, at man lever op til de krav, der kan stilles til sikker databehandling.

Datatilsynet har opstillet 12 minimumskrav for sikkerhed i forbindelse med *personaleadministration*. Principperne kan også anvendes i forbindelse med administration af *kundedata*.

1. **BESKRIVELSE**: Beskriv hvordan I beskytter jeres personaleoplysninger i personaleadministration og i praksis har implementeret pkt. 2-12. Beskrivelsen kan være særlige retningslinjer, der indgår i virksomhedens uddybende sikkerhedsregler, i en it-sikkerhedspolitik eller som en del af virksomhedens information til medarbejderne.

2. **ADGANG**: Adgang til oplysningerne skal begrænses til personer, der har et sagligt behov for adgang til oplysningerne. Det skal være så få personer som muligt.

3. **INSTRUKTION**: Medarbejdere, der håndterer personaleoplysninger, skal have instruktion og oplæring i, hvad de må gøre med oplysningerne, og hvordan de skal beskytte oplysningerne.

4. **PAPIRSFORM**: Personaleoplysninger på papir – f.eks. i kartoteker og ringbind – skal opbevares aflåst, når de ikke er i brug.

   Når dokumenter (papirer, kartotekskort mv.) med personaleoplysninger skal smides ud, skal der anvendes makulering eller anden foranstaltning, der forhindrer, at uvedkommende kan få adgang til oplysningerne.

5. **ADGANGSKODER**: Der skal anvendes adgangskode for at få adgang til pc'er og andet elektronisk udstyr med personoplysninger. Kun de personer, der skal have adgang, må få en kode.

   De personer, der har adgangskode, må ikke overlade koden til andre eller lade den ligge, så andre kan se den.

   Kontrol af tildelte koder skal foretages mindst en gang hvert halve år.

6. **LOGNING**: Det skal registreres, hvis der er forgæves forsøg på at få adgang til it-systemer med følsomme personaleoplysninger. Hvis der registreres et nærmere fastsat antal på hinanden følgende afviste adgangsforsøg, skal der blokeres for yderligere forsøg.

7. **USB-NØGLER**: Hvis personaleoplysninger lagres på en USB-nøgle, skal oplysningerne beskyttes. Der kan f.eks. bruges en USB-nøgle med adgangskode og kryptering. Ellers skal USB-nøglen opbevares i aflåst skuffe eller skab. Tilsvarende gælder ved opbevaring af personaleoplysninger på andre bærbare datamedier.

8. **VIRUSBESKYTTELSE**: PC'er koblet til internettet skal have en opdateret firewall og viruskontrol installeret.

9. **HJEMMESIDEFORMULARER**: Hvis der benyttes hjemmesideformularer, hvor følsomme personaleoplysninger og personnummer kan indtastes og fremsendes, skal der anvendes kryptering.

10. **E-MAIL:** Hvis følsomme personaleoplysninger og personnummer sendes med e-mail via internettet, anbefaler Datatilsynet kryptering.

11. **REPARATION OG SERVICE**: I forbindelse med reparation og service af dataudstyr, der indeholder

personoplysninger, og når datamedier skal sælges eller kasseres, skal der træffes de fornødne foranstaltninger, så oplysninger ikke kan komme til uvedkommendes kendskab.

12. **EKSTERN DATABEHANDLER**: Ved brug af en ekstern databehandler til håndtering af oplysninger, skal persondatalovens § 42 om skriftlig databehandleraftale mv. følges. Det gælder eksempelvis, når der anvendes et eksternt dokumentarkiv eller rekrutteringssystem på internettet.

3. Lever I op til de juridiske krav?

Det er et krav, at de juridiske forhold er i orden, dvs. aftaler / procedurer / persondatapolitikker.
Virksomhederne skal kunne dokumentere, at følgende forhold er opfyldte fra starten:

a. DATABEHANDLERAFTALER

b. SAMTYKKEERKLÆRINGER

c. ORIENTERINGSPLIGT – PERSONDATAPOLITIKKER (både intern og ekstern)

d. FORTEGNELSE OVER BEHANDLINGSAKTIVITETER

e. PROCEDURE FOR ANMELDELSE AF BRUD PÅ PERSONDATASIKKERHED

a. DATABEHANDLERAFTALER

Når virksomhedens data overføres til en ekstern databahandler, f.eks. et lønbureau eller et eksternt hotelmanagementsystem som f.eks. Techhotel skal der altid udarbejdes en databehandleraftale, hvis der overføres persondata fra jeres virksomhed til den eksterne databehandler.

Hvad er en databehandleraftale?

En aftale mellem jer og jeres databehandler (fx hostingvirksomhed).

Aftalen skal indeholde en beskrivelse af processen for behandlingen, formålet samt varigheden, herunder:

- beskrivelse af typer af data der behandles
- formålet med behandlingen
- varigheden af behandlingen
- kategorisering af de registrerede
- databehandlerens rettigheder og pligter
  (ikke utømmende oplistet).

Jeres eksterne databehandlere vil med stor sandsynlighed allerede have en databehandleraftale liggende, som I kan tage udgangspunkt i.

b. SAMTYKKEERKLÆRINGER

Vær opmærksom på, at der i visse tilfælde kræves samtykke fra den registrerede for behandling af oplysninger. Det gælder bl.a. behandlingen af personfølsomme data, men også behandling af personnummer og straffeoplysninger vil som regel kræve samtykke.

I skal derfor undersøge, om I har de nødvendige samtykker fra hhv. medarbejdere og kunder til behandling og opbevaring.

Personaleadministration
Ved ***personaleadministration*** kræves ikke samtykke til behandling af almindelige eller følsomme oplysninger, forudsat at behandlingen er nødvendig for at sikre jeres og medarbejderens forpligtelser og rettigheder, fx ved lønbehandling.

Der kræves derfor samtykke til alle registreringer og behandlinger, der ikke er nødvendige. I praksis er det som oftest følgende (ikke udtømmende angivet):

- Opbevaring af ansøgninger fra ansøgere, der har fået afslag på en stilling.
- Ved videregivelse eller indhentning af referencer.
- Ved anvendelse af medarbejderfoto på hjemmeside.
- Opbevaring af medarbejderkontrakter i mere end 5 år efter fratrædelse.

Eksempel på samtykkeerklæring

Medarbejderfotos

Jeg giver hermed samtykke til, at virksomheden kan anvende fotos af mig på virksomhedens hjemmeside.

Jeg er bekendt med, at jeg til enhver tid kan tilbagekalde mit samtykke. Sted og

dato:_____

_____
Medarbejderens navn og underskrift

Kundedata
Ved behandling af ***kundedata*** kræves ikke samtykke, hvis behandlingen er nødvendig for, at rettigheder kan fastlægges og gøres gældende. Det betyder, at man ikke må registrere unødvendige ting om sin kunde, fx personfølsomme oplysninger som etnicitet eller politisk overbevisning.

Hvis der er tale om en potentiel ny kunde, hvor der ikke tidligere har været nogen samhandel, kræves samtykke fra den registrerede dels efter persondataforordningen og dels efter markedsføringsloven (fx efter reglerne vedr. uanmodet henvendelse).

Reglerne for en samtykkeerklæring

Samtykke skal altid gives frivilligt, specifikt, informeret, og utvetydigt fra den registrerede.

FRIVILLIGT:	Felter på hjemmesiden må ikke være forhåndsudfyldt.
SPECIFIKT:	Det skal vedrøre et bestemt formål.
INFORMERET:	Eventuelle konsekvenser skal oplyses, og der skal oplyses om mulighed for at tilbagekalde samtykket.
UTVETYDIGT:	Letlæseligt og adskilt tydeligt fra anden tekst.

c. ORIENTERINGSPLIGT - PERSONDATAPOLITIK

I skal oplyse den registrerede person om de oplysninger, som I har liggende. Dette gælder både medarbejdere og fysiske kunder (ikke kapitalselskabskunder som fx et A/S eller ApS).

Der er **oplysningspligt** om følgende:

- Jeres navn og kontaktoplysninger
- Formålet med indsamlingen
- Det juridiske grundlag for indsamlingen
- Angivelse af hvem der berøres
- Angivelse af hvor dataene overføres til, fx tredjelande og retsgrundlaget for det (standardkontrakter som Privacy Shield- aftalen, SCC-aftalen mv.)
- Opbevaringstid
- Oplysning om ret til at tilbagekalde samtykke
- Retten til at klage til Datatilsynet
- Ved oplysninger fra tredjemænd: hvem disse tredjemænd er.

Oplysninger skal gives, inden behandlingen sker, medmindre den registrerede selv har afgivet oplysningerne.

Dette løses ofte ved at lave forskellige persondatapolitikker:

1. **a. En ekstern persondatapolitik**, der dækker virksomhedens kunder.

   b. **En cookie-politik** for besøgende på hjemmeside mv.

2. **En intern persondatapolitik**, der dækker medarbejderoplysninger.

Et ***eksempel på en intern persondatapolitik*** kunne være følgende (kan indsættes i virksomhedens personalehåndbog, idet den dog skal tilpasses konkrete forhold):

Intern persondatapolitik - medarbejderdata

Denne politik er udarbejdet for at oplyse om virksomhedens behandling af persondata vedrørende medarbejdere.
DATAANSVARLIG: Virksomheden er i personlovgivningens forstand dataansvarlig. Eventuel kontakt vedr. medarbejderdata kan ske til virksomhedens HR-afdeling.
FORMÅL: Der indsamles persondata omkring hver enkelt medarbejder. Persondata består i sædvanlige oplysninger vedr. medarbejderens forhold. Formålet for indsamlingen og behandlingen er personaleadministration. Oplysningerne stammer fra medarbejderen selv, fra medarbejdersamtaler og fra HR-afdelingen.
BEHANDLING OG HJEMMEL: Persondata i forbindelse med personaleadministration behandles i overensstemmelse med Datatilsynets retningslinjer. Der kræves ikke samtykke til behandling af disse oplysninger, så længe behandlingen er nødvendig for formålet. Ved brug af medarbejderfotos på hjemmeside kræves dog særskilt samtykke fra medarbejder, og dette samtykke kan til enhver tid tilbagekaldes.
OPBEVARING AF OG ADGANG TIL DATA: Persondata opbevares på ekstern server hos virksomhedens it-udbyder under forsvarlig sikkerhed. Desuden behandles oplysninger om løn hos virksomhedens lønstyringsbureau. Det er alene relevante ledere og HR-afdelingen, der har adgang til oplysningerne, foruden it-administratorer. Data opbevares som hovedregel i 5 år efter et ansættelsesforholds ophør. Ansøgninger fra kandidater, der ikke ansættes, opbevares som hovedregel i 6 måneder efter afslaget er givet.
RET TIL INDSIGT OG BERIGTIGELSE: Medarbejderen har ret til at få indsigt i og få berigtiget de persondata, som virksomheden ligger inde med. Snarest muligt og som hovedregel inden 4 uger efter modtagelsen af en begæring, skal oplysningerne udleveres. Når oplysninger er udleveret, kan medarbejderen tidligst anmode om tilsvarende oplysninger efter 6 måneder. Der kan ikke begæres indsigt i oplysninger, som findes at burde vige for offentlige eller private interesser, herunder hensynet til den pågældende selv.
KLAGE: Er en medarbejder ikke tilfreds med virksomhedens behandling af persondata, kan der klages til virksomhedens HR-afdeling. Medfører dette ikke afklaring, kan en eventuel klage herefter rettes til Datatilsynet. Den aktuelle kontaktadresse kan findes på www.datatilsynet.dk.

Denne politik suppleres af vores *eksterne persondatapolitik* vedrørende kundedata og henvendelse på hjemmeside. Der henvises også til virksomhedens it-politik.

d. FORTEGNELSE OVER BEHANDLINGSAKTIVITETER

Det hidtidige krav om anmeldelse til datatilsynet, hvis der behandles personfølsomme oplysninger ophører med Persondataforordningen. I stedet skal der i henhold til Persondatafordningen udarbejdes såkaldte fortegnelser, hvis virksomheden har mere end 250 ansatte *eller* behandler oplysninger, som medfører en høj risiko, dvs. hvis der behandles oplysninger, som kan være særligt sårbare for den registrerede hvis de slipper ud, f.eks. personlige forhold, eller hvis der behandles personfølsomme oplysninger.

Det anbefales under alle omstændigheder, at udarbejde sådanne fortegnelser, da det kan gøres i forbindelse med, at man alligevel skaffer sig overblik over sine datastrømme, og da fortegnelserne giver et godt overblik over de forskellige typer databehandling, som man har. Det kan og vil typisk være databehandlinger som f.eks. *Behandling af personaledata* og *Behandling af kundedata*.

Fortegnelsen skal bl.a. indeholde oplysninger om:

- Navn og kontaktoplysninger på den dataansvarlige
- Formålene med databehandlingen

- Kategorier af datasubjekter og datatyper
- Kategorier af modtagere af dataoplysninger
- Beskrivelse af overførsel til tredjelande
- Tidsfrister for sletning
- Overordnet beskrivelse af den tekniske og fysiske (organisatoriske) sikkerhed.

e. PROCEDURE FOR ANMELDELSE AF BRUD PÅ PERSONDATASIKKERHED

Ifølge persondataforordningen skal lækager og brud på persondatasikkerheden anmeldes til Datatilsynet inden 72 timer efter, at bruddet er konstateret.

Der skal gives anmeldelse om følgende forhold:

- Sikkerhedsbruddets karakter
- Konsekvenser ved bruddet
- Oplysning om hvordan skaden er (eller vil blive søgt) begrænset af den dataansvarlige
- Kontaktoplysninger på den dataansvarlige
- Fortegnelse over datahåndtering og andre relevante forhold op til sikkerhedsbrud, så myndighederne kan vurdere om forordningen er overholdt

Det anbefales at få lavet en procedure for håndtering af sådanne situationer.

Du er naturligvis altid velkommen til at kontakte HORESTA hvis du har spørgsmål om de nye regler eller om implementering af reglerne. SPØRGSMÅL kan rettes til:

Kaare Friis Petersen
Erhvervsjuridisk chef,
Erhvervsjura
Tlf.: +45 35 24 80 04/22 11 88 57
k.petersen@horesta.dk