

FAQ om persondata

Den 25. maj 2018 træder den EU's forordning om beskyttelse af persondata i kraft. Forordningens regler vil være direkte gældende i Danmark, men vil blive suppleret af regler i dansk lovgivning i form af en ny Databeskyttelseslov.

Forordningen indeholder enkelte helt nye regler og enkelte stramninger af allerede gældende regler, men langt de fleste regler, som vi kender dem fra Persondataloven, videreføres. Dog – og det er formentlig derfor forordningen har vakt så stor interesse – så hæves bødeniveauet markant, og der er derfor god grund til at få styr på persondatareglerne.

Nedenfor er anført en række ofte forekommende spørgsmål og svarene herpå. Denne FAQ supplerer den guide, som HORESTA har udarbejdet. Guiden kan læses her [\[link\]](#)

1. Hvilke oplysninger er omfattet af reglerne i persondataloven og forordningen?

ALLE oplysninger, som direkte eller indirekte kan identificere *en (fysisk) person* er omfattet af persondatalovgivningen. Det drejer sig f.eks. om navn, adresse, cpr.nr., e-mailadresser, telefonnumre, IP-adresser, betalingskortoplysninger, helbredsoplysninger, sociale oplysninger, strafoplysninger, billeder, videooptagelser, stemmeoptagelser, fingeraftryk (og andre biometriske data), en bils reg.nr. osv. Det afgørende er ikke nødvendigvis om man selv ud fra informationen – f.eks. en bils reg.nr. - kan identificere en fysisk person, men at nogen kan.

Oplysninger om et firma eller et selskab (A/S eller ApS) er ikke omfattede. F.eks. vil generelle mailadresser på virksomheder/selskaber, som f.eks. info@xxxxxx.dk ikke være omfattet.

2.. Hvad betyder det at "behandle" oplysninger?

"Behandling" af oplysninger dækker ALLE handlinger vedr. persondata, herunder indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfindning, søgning, brug, videregivelse, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

3. Hvad er en "dataansvarlig"

Man er »dataansvarlig«, som person eller virksomhed, hvis man alene eller sammen med andre står for indsamling af persondata, og bestemmer til hvilke formål og med hvilke hjælpemidler indsamlede persondata skal behandles.

4. Hvad er en databehandler?

En »databehandler« er den person eller virksomhed, som alene behandler persondata *efter ordre* fra den dataansvarlige. En databehandler foretager således ingen selvstændig behandling af oplysningerne, men alene den behandling, som han får besked om fra den dataansvarlige. Et eksempel på en ekstern databehandler kan være "Spectra", som leverer systemer til booking og registrering af gæster.

Hvis du anvender eksterne databehandlere, skal du altid have en såkaldt "Databehandleraftale", som bemyndiger den pågældende databehandler til at behandle persondata på dine vegne, og som tager stilling til præcis hvilken behandling databehandleren er bemyndiget til.

5. Hvornår må jeg bede om at få personoplysninger?

Du skal have en legitim, dvs. en saglig grund/formål, til at bede om at få personoplysninger, og du skal have hjemmel i loven til at indhente oplysninger. En saglig grund er f.eks., at en person er gæst på hotellet. Her kan du bede om alle de personoplysninger, såsom navn, fødselsdato, nationalitet, fast bopæl, ankomstdato og type af og nummer på pas eller anden rejselegitimation, som du har brug for til at opfylde aftalen. Det samme gør sig gældende i forhold til f.eks. ansættelsesforhold, her vil du også, som arbejdsgiver, have brug for en række personlige oplysninger for at ansættelsesforholdet kan etableres og opretholdes. Nogle oplysninger kan du bede om uden videre, mens du skal have samtykke til andre oplysninger, se mere herom nedenfor under spgm. 7 og 8.

Du kan bede om personlige oplysninger, såfremt:

- Det er til brug for en aftale, f.eks. et kundeforhold men også en ansættelseskontrakt
- Du er forpligtet til det efter loven, f.eks. skal hoteller anmode gæster om en række oplysninger i forbindelse med check in
- Du har en "berettiget" interesse i at få de pågældende oplysninger, og hensynet til den registrerede/personen ikke overstiger denne interesse
- Hvis du har samtykke fra personen. I nogle tilfælde skal man have samtykke fra personen

6. Hvilke oplysninger må jeg bede om?

Indenfor persondataretten, gælder et såkaldt dataminimeringsprincip, som groft sagt betyder, at du ikke må bede om flere oplysninger, end du har brug for. Du må altså ikke bede om

oplysninger, som du *tror* du kan få brug for, men kun oplysninger, som du *ved*, og kan dokumentere, at du har brug for.

I en ansættelsessituation skal du f.eks. vurdere, om du i forbindelse med den konkrete ansættelse har brug for at få straffeattest fra den pågældende. Hvis du beder om en straffeattest SKAL du under alle omstændigheder have et samtykke fra den pågældende, men du skal også kunne argumentere, at du har et legitimt behov for denne oplysning, jf. spgm. 1 overfor. Det kan f.eks. være, at den pågældende skal forvalte pengebeløb, eller skal have adgang til gæsternes værelser. Her vil det være relevant at vide, om den pågældende er tidl. straffet for f.eks. tyveri, mens dette ikke vil være relevant for en opvasker i køkkenet.

7. Hvad er forskellen på almindelige personoplysninger og personfølsomme oplysninger?

Som såkaldt *personfølsomme oplysninger* anses oplysninger om:

- Race eller etnisk oprindelse
- Politisk, religiøs eller filosofisk overbevisning
- Fagforeningsmæssigt tilhørsforhold
- Genetiske og biometriske forhold
- Helbredsoplysninger
- En persons seksuelle forhold eller seksuelle orientering

Alle andre oplysninger anses for at være "almindelige" oplysninger. Dog er der særlige regler omkring strafoplysninger, CPR.nr. og fagforeningsmæssigt tilhørsforhold, se nedenfor under spørgsmål 8.

For at bede om personfølsomme oplysninger skal *særlige grunde være opfyldt*, herunder f.eks. hvis oplysningerne er nødvendig for at fastlægge eller gøre et retskrav gældende eller forsvare dette, Personfølsomme oplysninger kan også indhentes, hvis man får den pågældendes samtykke, men man skal dog stadig sikre sig, at man har et legitimt formål med at bede om de personfølsomme oplysninger, jf. spgm. 5 og 6.

Behandlingen af personfølsomme oplysninger bør altid ske med en høj grad af sikkerhed, og i henhold til den nye persondataordning nævnes det, at videresendelse af personfølsomme oplysninger bør (skal) krypteres i forbindelse med forsendelsen. Det kan f.eks. være, hvis et medlem har en personalesag, hvori der indgår personfølsomme oplysninger, og man ønsker at videresende disse oplysninger til HORESTA eller en anden rådgiver. Det kan f.eks. være, at virksomheden skal fremsende en lægeerklæring.

8. Hvilke oplysninger SKAL jeg have samtykke til at indhente fra ansatte

Du skal altid have samtykke til at indhente straffeattest og til at bruge billeder af dine ansatte, uanset om der er tale om billeder, som lægges ud på en medarbejderoversigt eller, om der er tale om billeder, som skal bruges i virksomhedens markedsføring, f.eks. til brug for en brochure. Her vil det være en god ide at få et samtykke, som betyder, at billed(markedsførings)materiale, hvor medarbejderens billede indgår, også kan bruges efter medarbejderens fratræden. Derudover vil du – medmindre en af de undtagelsesgrunde som er nævnt i forordningen gør sig gældende - skulle bede om samtykke, hvis du beder om personfølsomme oplysninger, jf. spgm. 7 ovenfor.

For så vidt angår medarbejdere, skal du ikke have samtykke til at bede om CPR.nr., da det følger af skattelovgivningen, at du skal indhente dette fra medarbejderne.

Du vil også skulle bede om samtykke til at indhente oplysninger om en medarbejders eventuelle fagforeningsmæssige tilhørsforhold, *medmindre* du i din virksomhed har overenskomst. Så kan du bede om oplysningerne uden samtykke.

9. Hvilke oplysninger skal jeg have samtykke til at indhente fra kunder eller andre

Hvis du ønsker, eller har brug for, at indhente/registrere og bruge personfølsomme oplysninger om gæster eller andre personer, som virksomheden har relationer til, vil dette kræve samtykke fra den/de pågældende, jf. om spgm. 7. Som anført skal man – udover at sikre sig et samtykke – *meget nøje* kunne redegøre for, hvilke saglige/legitime grunde, der ligger bag registrering og behandling af personfølsomme oplysninger. At indhente og/eller registrere personfølsomme om andre end ansatte vil generelt vanskeligt kunne begrundes sagligt.

Det vil også kræve samtykke, hvis du beder om personnummer fra kunder eller andre fysiske personer, f.eks. leverandører. Det vil i øvrigt, som udgangspunkt, ikke tjene et "legitimt" formål at bede kunder/leverandører om CPR.nr., medmindre der er tale om et løbende/langvarigt kundeforhold.

10. Skal et samtykke være skriftligt?

Nej, der er ikke lovkrav om at et samtykke *skal* være skriftligt, men der er i forordningen krav om, at et samtykke skal være *udtrykkeligt*. Da det er dig som dataansvarlig, som skal bevise, at der er indhentet samtykke til f.eks. brug af en medarbejders billede. Det er derfor en rigtig god ide altid at sikre sig, at et samtykke er skriftligt. Man kan f.eks. indarbejde det som en del af ansættelsesaftalen.

11. Er der andre krav til et samtykke?

Ja, et samtykke skal være klart, forståeligt og frivilligt. Det betyder f.eks. at et samtykke ikke må "skjules" i en længere tekst, og at det skal være forståeligt for den pågældende, hvad han/hun giver samtykke til, dvs. hvorfor der gives samtykke og hvad oplysningerne vil blive brugt til. At et samtykke er frivilligt betyder, at en aftale – som udgangspunkt – ikke må betinges af, at der gives et samtykke, medmindre de oplysninger, der bedes om, er *nødvendige* for at opfylde aftaleforholdet. Det sidstnævnte forhold er bl.a. begrundelsen bag, at man skal vurdere, om det "nødvendigt" at indhente oplysninger om strafforhold for en ansat, jf. spgm. 6.

12. Hvad må jeg bruge indhentede personoplysninger til?

Du må bruge de indsamlede oplysninger til det formål, som de er indhentet til, og til formål, som ikke er *uforenelige* med det oprindelige formål. Hvis nogle af de personoplysninger, som man behandler, er indhentet efter samtykke, må oplysningerne alene anvendes til det, som der specifikt er givet samtykke til.

For så vidt angår oplysninger om medarbejdere har Datatilsynet udtalt, at sådanne oplysninger *alene* kan anvendes til brug for ansættelsesforholdet, man kan altså ikke f.eks. videregive oplysninger om medarbejdere til andre arbejdsgivere, medmindre man får medarbejderens samtykke hertil.

Området for at anvende personoplysninger til andet, end det de er indhentet til, er snævert, og det vil bero på en konkret vurdering. Et eksempel på, at oplysninger blev brugt til et formål, som *ikke* var foreneligt med det oprindelige formål var en sag om en natklub A, som havde et kunderegister med kunder, som modtog nyhedsbrev og info fra klubben.

På et tidspunkt blev virksomheden overdraget til et ApS, B, som også fik adgang til kunderegisteret. Her fandt Datatilsynet, at videregivelsen af oplysningerne til B var uforeneligt med det oprindelige formål, som var, at A (og ikke B) kunne udsende tilbud mv. Et andet eksempel på et ikke foreneligt formål var en tandlæge, som anvendte sit kunderegister til at udsende valgmateriale til sine klienter i forbindelse med, at han stillede op til kommunalvalget.

13. Må jeg bruge kundeoplysninger til markedsføring og udsendelse af nyhedsbreve?

For så vidt angår kundeoplysninger, kan det være legitimt at anvende en gæsts e-mailadresse til brug for markedsføring af egne *tilsvarende* ydelser, som den gæsten har købt, f.eks. en overnatning. Dette forudsætter dog, at reglerne herom i markedsføringslovens § 10 er overholdt. Det vil bl.a. sige, at kunden skal informeres om, at f.eks. en e-mailadresse *kan* blive anvendt til markedsføring, og kunden skal efterfølgende have mulighed for at frabede sig dette. Desuden skal kunden også let og enkelt efterfølgende kunne framelde sig denne markedsføring.

Mht. udsendelse af nyhedsbreve forudsætter dette gæstens samtykke.

14. Hvor længe må jeg gemme personoplysninger?

Dette er det oftest stillede spørgsmål, og hverken forordningen eller loven giver noget konkret svar herpå.

Helt generelt må man gemme oplysninger, *så længe det er nødvendigt til de formål, som oplysningerne blev indsamlet til*. Det helt klare udgangspunkt er altså, at personoplysninger skal slettes, når man ikke længere skal bruge dem til det formål, som de blev indhentet til. Man kan altså ikke gemme gæsteoplysninger over længere tid blot fordi, man har en formodning om, at gæsten måske kommer igen, medmindre gæsten har givet samtykke hertil, f.eks. som led i et loyalitetsprogram.

Efter hhv. Udlændingebekendtgørelsen og Pasbekendtgørelsen skal man dog gemme gæsteoplysninger i ét år, jf. spgm. 15 nedenfor, men dette er alene med det formål, at kunne stille oplysningerne til rådighed for Politiet. Jf. spgm. 13 ovenfor kan det dog være legitimt at gemme en gæsts e-mailadresse i længere tid med henblik på at sende gæsten tilbud om f.eks. overnatning.

Man må også gerne gemme oplysninger i længere tid, hvis de alene anvendes til statistiske formål, men i så fald skal oplysningerne anonymiseres.

Hvorvidt personoplysninger kan gemmes over længere tid beror på en konkret vurdering af, om opbevaringen heraf tjener et *legitimt* formål. Det kan f.eks. være legitimt i en periode at gemme oplysninger om jobansøgere, som ikke fik det opslåede job, f.eks. for at kunne imødegå eventuelle indsigelser om diskrimination. Man kan også bede om samtykke til at gemme oplysningerne, med henblik på at kontakte den pågældende i forbindelse med et fremtidigt jobopslag.

Når en medarbejder er fratrukket, kan det være legitimt, at gemme personalemappen i en længere periode for at kunne imødegå eventuelle efterfølgende krav om efterbetalinger fra fratrukkede medarbejdere. Efterbetalingssager er undergivet en 5 årig forældelse og krav kan således rejses 5 år tilbage.

Hvis man gemmer personaleoplysninger i en længere periode, skal man være opmærksom på, at man kun gemmer de oplysninger, som man kan for brug for. Øvrige oplysninger skal slettes.

15. Er der oplysninger jeg skal gemme?

Efter regler i hhv. Udlændingebekendtgørelsen og Pasbekendtgørelsen skal hoteller registrere forskellige oplysninger om gæsterne. For udenlandske gæsters vedkommende skal disse oplysninger gemmes i min 1 og max 2 år, mens de for danske gæster skal gemmes i 1 år.

16. Hvad med regnskabsoplysninger?

Det følger af bogføringsloven, at bogførings/regnskabsmateriale skal gemmes i en periode på 5 år, herunder f.eks. genparten af fakturaer, som kan indeholde personoplysninger. Hvilket materiale, der er omfattet af denne pligt, fremgår specifikt af lovens § 3.

17. Hvilke oplysninger skal jeg give gæster og medarbejdere?

I forbindelse med indsamlingen af personoplysninger er der pligt til at give en række oplysninger til de personer, som du registrerer, dette uanset om det er kunder eller medarbejdere. Det drejer sig i punktform om flg. oplysninger:

1. Din identitet som dataansvarlig og dine kontaktoplysninger
2. Formålene med den behandling, som personoplysningerne skal bruges til, og retsgrundlaget for behandlingen
3. De legitime interesser, som du har i at behandle oplysningerne
4. Hvis oplysninger videresendes til andre, da eventuelle modtagere eller kategorier af modtagere af personoplysningerne
5. Det tidsrum, hvor personoplysningerne vil blive opbevaret, eller hvis dette ikke er muligt, de kriterier, der anvendes til at fastlægge dette tidsrum
6. Retten til at anmode den dataansvarlige om indsigt i og berigtigelse eller sletning af personoplysninger og retten til at gøre indsigelse mod behandling samt retten til dataportabilitet, dvs. retten til at få sine personoplysninger overført til en anden dataansvarlig
7. Retten til at trække samtykke tilbage på ethvert tidspunkt
8. Retten til at indgive en klage til en tilsynsmyndighed
9. Orientering om, hvorvidt behandlingen af personoplysninger er lovpligtigt eller et krav i henhold til en kontrakt eller et krav, der skal være opfyldt for at indgå en kontrakt, samt om den registrerede har pligt til at give personoplysningerne og de eventuelle konsekvenser af ikke at give sådanne oplysninger
10. Orientering om, hvorvidt oplysningerne anvendes til "profilering", dvs. f.eks. til at kategorisere en kunde.

18. Hvilke rettigheder har kunder og medarbejdere vedr. de registrerede oplysninger?

Når du behandler persondata, uanset om det er oplysninger vedrørende medarbejdere eller kunder, så skal du være opmærksom på, at de pågældende har en række rettigheder, som

du, som dataansvarlig, på ethvert tidspunkt skal kunne imødekomme. Det drejer sig om følgende:

1. Retten til at blive oplyst om formålene med behandlingen
2. Retten til at blive oplyst om, hvilke personoplysninger, der behandles
3. Retten til at få oplyst, hvilke modtagere eller kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til
4. Retten til at få oplyst det påtænkte tidsrum, hvor personoplysningerne vil blive opbevaret
5. Retten til at anmode den dataansvarlige om berigtigelse eller sletning af personoplysninger eller begrænsning af behandling af personoplysninger vedrørende den registrerede eller til at gøre indsigelse mod en sådan behandling
6. Retten til at indgive en klage til en tilsynsmyndighed
7. Retten til information om, hvorfra personoplysningerne stammer, hvis de *ikke* indsamles hos den registrerede
8. Retten til at få viden om oplysningernes anvendes til "profilering" og konsekvenserne heraf

19. Hvordan skal jeg i praksis kunne give de lovpligtige informationer og imødekomme kunder og medarbejders rettigheder?

Det kan forekomme overvældende, at skulle give alle de informationer, som er nævnt ovenfor under spgm. 16 og 17, og det vil da også i praksis være umuligt overfor f.eks. en telefonisk kunde at give alle de nævnte informationer i telefonen.

KUNDER

I praksis bør alle virksomheder, som behandler persondata derfor, i forhold til deres kunder, udarbejde en "Privacy Policy" eller en persondatapolitik. Af denne policy bør de nævnte informationer, f.eks. vedr. behandling af kundedata fremgå, og det bør også fremgå, hvilke rettigheder de registrerede kunder/gæster har.

Hvis gæsten booker elektronisk, bør der være en klar og tydelig henvisning til virksomhedens privacy policy, og -hvis muligt - bør gæsten f.eks. i en klikboks klikke af, at han/hun er bekendt med denne policy, dette er dog ikke et lovkrav. For så vidt angår andre former for booking, bør virksomhedens Privacy Policy fremgå af f.eks. den bekræftelse på en booking, som gæsten modtager. Virksomhedens Privacy Policy bør også have en fremtrædende/tydelig plads på virksomhedens hjemmeside.

MEDARBEJDERE

For så vidt angår medarbejdere bør de nævnte informationer fremgå af en medarbejderhåndbog, som der henvises til i ansættelseskontrakten, eller i et tillæg til kontrakten.

For så vidt angår ansøgere til en stilling, bør de pågældende have de nævnte informationer i forbindelse med tilbagemeldingen fra virksomheden. Der kan i den forbindelse udarbejdes en standardskrivelse, som sendes med ud til ansøgerne. Det vil alene være nødvendigt at informere de ansøgere, som man går videre med, medmindre man gemmer de øvrige ansøgninger til senere brug.

Frederiksberg 27.10.2017/Kfp