



Bliv klar til EU's Persondataforordning GDPR

Er i klar til de nye regler?

Øget ansvar, mere dokumentation og markant højere bødestrafte er blandt hovedpunkterne i EU's Persondataforordning - General Data Protection Regulation (GDPR), der træder i kraft i 2018. Men ifølge Danske IT Advokater er ganske få klar til at implementere de nye regler.

CapaSystems har lavet tjeklisten, der gennemgår, hvad I skal være opmærksomme på – og hvordan I kan blive klar til de nye, omfattende regler. Du kan på en enkel måde få et overblik over virksomhedens status ved at tælle point sammen for hvert spørgsmål og se det endelige resultat sidst i denne tjekliste.



Er I klar til EU's Persondataforordning (GDPR)? I så fald tilhører I et mindretal...

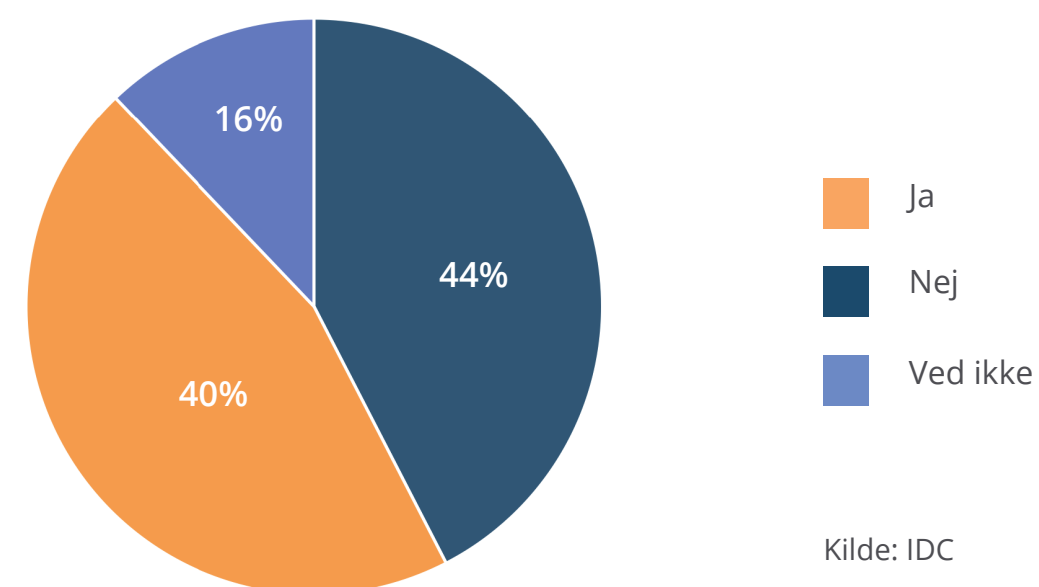
Næsten hver femte virksomhed, som IDC har spurgt i deres undersøgelse, har ikke engang hørt om EU's Persondataforordning.

40% har kendskab til EU's Persondataforordningen

Er din virksomhed klar til GDPR?

Det spørgsmål svarer 44% af virksomhederne ja til. 40% svarer nej og 16% svarer ved ikke.

Klar til EU's Persondataforordning



Med godt seks måneder til den nye forordning træder i kraft, er det måske oplagt at tænke, at der er masser af tid til, at du kan sætte dig ind i reglerne. Men her får du 4 gode grunde til ikke at udsætte processen et sekund længere.

4 grunde til, at du skal forberede din virksomhed på GDPR nu

Persondataforordningen vedrører virksomheder, der indsamler og / eller behandler data, der kan henføres til borgere i EU. Dette gælder også selvom data er forsøgt anonymiseret ved hjælp af indirekte nøgler.

1. **Den nye forordning stiller store krav til jeres dokumentation** – I skal blandt andet udarbejde privatlivspolitikker, nedskrive procedurer for, hvordan I håndterer rettigheder m. m.
2. **Reglerne kræver engagement og nye processer** – Efterlevelsen af de nye regler skal ind under huden på alle ansatte og indarbejdes i nye processer. Det kræver engagement fra top til bund i hele virksomheden.
3. **Nødvendig kortlægning** – Før I overhovedet kan tænke på dokumentation og nye processer, skal data og datastrømme kortlægges.
4. **I får brug for at prioritere** – Med mere end 99 artikler og ca. 125 siders lovstof fra EU, får I brug for at prioritere jeres fokus og indsats.



EU's Persondataforordning – kort fortalt

Persondataforordningen træder i kraft 25. maj 2018. Ifølge Dansk IT vil det tage virksomheder op til 18-24 måneder at indrette sig, så de kan opfylde de nye regler.

Men hvad går forordningen ud på? Forordningen erstatter loven om beskyttelse af persondata fra 2001.

Selvom mange af principperne for databehandling grundlæggende er de samme som i den nye persondataforordning, så har nye måder at indsamle data digitalt, f.eks. på de sociale medier, gjort det nødvendigt at øge beskyttelsen af borgerne i EU.

Det ses blandt andet af bødestørrelserne – op mod 4% af den årlige globale koncernomsætning eller 20 mio. EUR (hvad end der er højest) – har påkaldt sig stor opmærksomhed.

Kerneprincipper i EU's Persondataforordning

1. Skærpede krav til samtykke
2. Retten til som person at blive glemt
3. Øgede dokumentationskrav
4. Notifikationspligt
5. For nogle virksomheder bliver det et krav at udpege en Data Protection Officer (DPO)
6. Databeskyttelse gennem design og standardindstillinger
7. Skærpede krav til brug af eksterne databehandlere

GDPR gælder for alle virksomheder, der:

behandler personoplysninger for kunder, medarbejdere, kontakter mv. Herunder navne, postadresser, mailadresser, IP-adresser samt følsomme oplysninger som f.eks. CPR-numre, politisk, filosofisk eller religiøs overbevisning

tilbyder varer eller tjenester til EU-borgere og behandler deres data (uanset hvor virksomhedens hovedsæde er placeret). Det er dataejer, som er ansvarlig - uanset om det er en ekstern leverandør, som indsamler og behandler data

Dermed vil de fleste virksomheder skulle gøre sig klar til at efterleve de nye regler, og som minimum skal I have klarhed over, hvorvidt I er omfattet.

Brug forordningen som en løftestang

For mange virksomheder vil EU's nye persondataforordning betyde, at der skal sættes timer af til at kortlægge applikationer, it-services og data, dokumentere hvordan data behandles og udarbejde samt indoperere nye processer.

Derfor anbefaler CapaSystems, at I bruger forordningen som en løftestang til at få:



større
indsigt i data



bedre
sikkerhedsprocedurer



effektiviserede og
strømlinede processer

I sidste ende handler det om beskyttelse af kunders og medarbejderes data – og de nye regler for persondata kan ses som en anledning til at få bedre styr på sikkerheden.

Ny persondataforordning eller ej - sikkerhedshuller kan koste dyrt; både på bundlinjen og i forhold til tab af omdømme og tillid.

Tjekliste til EU's Persondataforordning 2018

7 spørgsmål, der klæder jer bedre på til at håndtere EU's nye regler for persondata

1.

Hvor forankret er kendskabet til – og bevidstheden om – EU's nye persondataforordning i virksomheden?

De højere bøder, behovet for nye procedurer, og eventuel udpegelse af dataansvarlige og databehandlere, bevirker, at manglende kendskab til – eller efterlevelse af forordningen – kan få afgørende indflydelse på virksomhedens virke.

Så på en skala fra 1-5, hvor godt forankret er kendskabet til EU's Persondataforordning i jeres virksomhed?

1	2	3	4	5
Hverken jeg eller andre i virksomheden har kendskab til EU's Persondataforordning	Jeg mindes at have hørt noget, men det er længe siden	Vores IT-afdeling har fokus på de nye regler	Ledelsen samt IT har fokus på reglerne	Vi er i gang med at forberede / har allerede initiativer og regelsæt, så virksomheden efterlever forordningen

2. I hvilket omfang har I kortlagt de persondata, virksomheden behandler?

Selvom de grundlæggende principper for behandling af persondata er de samme som i den nuværende persondatalov, vil de fleste virksomheder have behov for at kortlægge, hvilke persondata der skal behandles samt i hvilke systemer, de befinder sig og hvem der har adgang til data og så videre.
Det betyder, at I skal kunne besvare følgende spørgsmål som led i jeres kortlægning.

Markér i hvor høj grad I har kortlagt følgende områder af jeres behandling af persondata (hvor 1 angiver, at I endnu ikke er startet, og 5 at I har kortlagt området):

1. Typer af persondata virksomheden indsamler	1	2	3	4	5
2. Hvor data indsamles fra	1	2	3	4	5
3. Hvordan data indsamles	1	2	3	4	5
4. Hvor og hvordan oplysninger er sikret	1	2	3	4	5
5. Hvordan oplysninger bruges nu og hvordan de tænkes brugt i fremtiden	1	2	3	4	5
6. Hvornår og hvordan vil oplysningerne blive slettet?	1	2	3	4	5
Sum					



Hvad er "behandling" af persondata?

Måske sidder du lige nu og tænker, hvad ligger der egentlig i begrebet "behandling af persondata" i forhold til EU's Persondataforordning (GDPR).
Ifølge direktivet betyder behandling: "Indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfindning, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse." Kilde: DI Digital

3. I hvilken grad har I prioriteret jeres indsatsområder?

EU's Persondataforordning vil påvirke danske virksomheder i forskelligt omfang, alt efter deres forretning. Derfor giver det mening at identificere og prioritere, hvilke dele af persondataforordningen, der får størst indflydelse på jeres forretning.

Her skal I blandt andet være opmærksomme på at få prioriteret nye tiltag og procedurer, hvor forordningens regler griber ind i produksalg mv. Der gælder f.eks. særlige regler for apps m. m., der indsamler personoplysninger fra personer under 16 år, ifølge LETT Advokater.

I hvilken grad har I prioriteret, hvor persondataforordningen får forretningsmæssig betydning for jer?

1	2	3	4	5
Slet ikke	I lav grad	I nogen grad	I høj grad	I meget høj grad



Tip

DI Digital (Dansk Industri) ser beskyttelsen af persondata som et afgørende konkurrenceparameter for virksomheder fremadrettet.
De har udarbejdet en omfattende skabelon for beskyttelse af persondata, som kan [læses her](#)

4. I hvor høj grad har I afdækket risici?

DI Digital anbefaler, at virksomheder gennemfører en risikoanalyse med fokus på, hvor der er størst risici forhold til behandlingen af persondata – og herefter iværksætter de nødvendige sikkerhedstiltag. I skal blandt andet vurdere, om I skal have kryptering og pseudonymisering, samt hvordan I vil håndtere datanedbrud.

Så, hvor langt er I med risicivurdering samt eventuelle sikkerhedstiltag?

1	2	3	4	5
Vi har ikke vurderet risici ved databehandlingen	Vi har vurderet risici i forbindelse med behandling af persondata, men det er over tre år siden	Vi har vurderet risici i forbindelse med behandling af persondata, men det er over tre år siden	Vi er i gang med at vurdere risici ved behandling af persondata	Vi har gennemført en risicivurdering og har allerede / har igangsat sikkerhedstiltag



Husk!

Oplever I et sikkerhedsbrud, der involverer persondata, skal Datatilsynet have besked indenfor 72 timer, hvor I skal kunne fortælle om type af datanedbrud, typer af berørte data, antal registrerede, konsekvenser for de berørte mv. Derfor kræver det analyse, procedurer og dokumentation på forhånd.

5. Hvor godt har I dokumenteret jeres sikkerhed i forbindelse med behandling af persondata?

En af de nye tiltag ved EU's Persondataforordning (GDPR) er større krav til dokumentation. Det gælder blandt andet udarbejdelse af privatlivspolitikker, nedskrevne procedurer til hvordan I håndterer registreredes rettigheder samt generel dokumentation, der viser, at I overholder forordningens regler.

Det betyder, at I skal udarbejde dokumentation for blandt andet forretningsprocesser samt forretningsgange. Start med at danne jer et overblik over, hvilken dokumentation I allerede har i dag og afdæk så, om I har brug for yderligere dokumentation.

Markér i hvor høj grad I har dokumenteret følgende (hvor 1 angiver i ringe grad, og 5 angiver i høj grad):

1. IT-sikkerheden er blevet gennemgået og dokumenteret	1	2	3	4	5
2. Der er udarbejdet en beskrivelse for håndtering af eventuelle sikkerhedsbrister	1	2	3	4	5
3. Der findes en generel beskrivelse af de registreredes rettigheder	1	2	3	4	5
4. Der findes procesbeskrivelser for håndtering af indsigtsanmodninger, anmodninger om sletning eller berigtigelse fra de registrerede	1	2	3	4	5
Sum					



Med PerformanceGuard kan du

- gøre virksomheden i stand til selv at få overblikket
- indsamle og levere den data, der kan spare virksomheden for dyre GDPR-konsulenter
- levere det fulde overblik over brugen af ALLE applikationer og IT-services - interne såvel som eksterne

6. Har I en sikkerhedsansvarlig?

Som led i EU's Persondataforordning skal virksomheder, der som kerneaktivitet behandler persondata eller som behandler følsomme personoplysninger i større omfang, udpege en Data Protection Officer (DPO). DPO'en skal have særlig viden om persondatabeskyttelse og sikre, at reglerne overholdes.

Men uanset om I, ifølge forordningen, skal udpege en DPO, anbefaler Dansk Industri og Ministeriet for Videnskab, Teknologi og Udvikling samt DI Digital, at virksomheder udpeger en IT-sikkerhedsansvarlig, der sørger for alt fra at koordinere til at dokumentere og agere i forhold til sikkerhedspolitikker, -procedurer eller -brud.

Har I en sikkerhedsansvarlig eller DPO?

1	5
Nej	Ja



Hvad er en DPO?

En nyskabelse i EU's Persondataforordning er kravet til virksomheder, der behandler følsomme personoplysninger – om at udpege en Data Protection Officer (DPO) – eller databeskyttelsesrådgiver.

”En person, der har det som sin opgave at sikre beskyttelse af personoplysninger og efterlevelse af reglerne”. Kilde: DI Digital

7. Hvor gode er jeres sikkerhedsprocedurer?

Betragter I kunders og medarbejderes data som et aktiv, som I kontinuerligt arbejder for at beskytte mod nedbrud eller angreb?

Opdatering af software, beskyttelse af passwords, antivirussoftware, firewalls, logfiler og back-ups bør være en fast del af jeres sikkerhedsprocedurer.

Persondataforordningen kræver, at virksomheder fastsætter gennemsigtige sikkerhedspolitikker og -procedurer, så brug forordningen som en løftestang til at få 110% styr på sikkerheden.

Markér i hvor høj grad jeres sikkerhedsprocedurer er up-to-date (hvor 1 angiver i ringe grad, og 5 angiver i høj grad):

1. I har overblik over hvilke typer software I er i besiddelse af, og har dokumenteret, hvordan det er konfigureret	1	2	3	4	5
2. I har en rutine eller procedurer for hvornår, der offentliggøres nye trusler og IT-baserede opdateringer til softwaren	1	2	3	4	5
3. I tager back-up af alle data og systemer på en struktureret måde	1	2	3	4	5
4. I har udpeget en person, der hver dag læser de logfiler, der er af størst betydning	1	2	3	4	5
Sum					



Med CapaInstaller kan du

- sætte security level på devices, herunder passcode og kryptering
- sætte policy management på devices
- få information om device versioner
- styre system opdateringer
- få information om manglende opdateringer
- få information om installeret software

Hvor godt er i klædt på?

Optæl dine point og se hvor godt I er klædt på til at håndtere EU's Persondataforordning (GDPR).

Score	Niveau
20-30	I er vist ikke helt kommet ud af starthullerne
30-45	I er så småt i gang med opvarmningen
45-60	I har krydset startlinjen og passeret 5 kilometers mærket i fin stil
60-85	I kan se mållinjen forude
85-	I er en sikker vinder og rollemodel for alle os andre

Hvis du ikke scorede så højt, som du havde håbet, så fortvivl ikke. Du ved allerede mere end mange andre – og er godt i gang med at sætte dig ind i emnet.



Næste skridt

Du har fået ny viden og har gennemgået vores tjekliste.
Vil du vide, hvordan du kommer nemt i gang med at implementere sikkerhedstiltag, nye processer og procedurer – uden at hæmme virksomhedens effektivitet?

Så er du velkommen til at kontakte os.

Vi giver gerne en uforpligtende analyse af, hvordan CapaSystems' software kan understøtte jer på vejen mod større sikkerhed – uden at gå på kompromis med fleksibilitet eller medarbejdernes arbejdsglæde.

[Kontakt os og hør nærmere](#)



Om Capasystems

CapaSystems har leveret effektive og brugerorienterede softwareløsninger siden 1996. 60 dedikerede medarbejdere står bag udviklingen af softwaren CapaInstaller og PerformanceGuard. Vores mål er at give jer bedre overblik, lavere omkostninger og større brugertilfredshed. Vi gør det med ekspertise og smart software, der effektiviserer processer for alle vores kunder. Vi lever for automatisering af IT-løsninger. Vores vision er en fremtid, hvor smarte teknologier eliminerer alle manuelle processer.

Så får I mere tid på kontoen!

Kilder

Dansk Erhverv, It og sikkerhed, <http://www.danskerhverv.dk/MinBranche/Raadgivning-videnservice/itogteknologi/Sider/forside.aspx>

DI, De ti vigtigste IT-sikkerhedsinitiativer, <https://di.dk/SiteCollectionDocuments/Downloadboks%20-%20lokale%20filer/Down-lads%20lokale%20filer%2005-08/ITSikkerhedGoderaadITEKDI.pdf>

Ibiz.center, It-sikkerhed, <https://www.ibiz-center.dk/viden-om-it/trends-og-muligheder/sikkerhed/>

IT-Branchen, Sådan får du styr på persondataforordningen, <https://itb.dk/news/it-sikkerhed/s%C3%A5dan-f%C3%A5r-du-styr-p%C3%A5-persondataforordningen>

Horten, Persondataforordningen er klar, <http://www.horten.dk/Nyhedsliste/2015/December/Persondataforordningen-er-klar-stoerre-kontrol-over-egne-data-og-hoejere-boeder>

LETT Advokatpartnerselskab, Sådan forbereder du din organisation på persondataforordningen, <http://www.lett.dk/viden/faglige-nyheder/faglige-nyheder-2016/saadan-forbereder-du-din-organisation-paa-persondataforordningen>

Version2, Hver anden virksomhed kender ikke persondataforordningen: <https://www.version2.dk/artikel/hver-anden-virksomhed-kender-ikke-til-persondataforordningen-de-har-travlt-836314>

DANSK IT, Sådan forbereder du dig på persondataforordningen, https://dit.dk/da/DANSKITmener/Nyheder/Persondataforordning_anbefalinger

Version2, Skrappe persondata-regler på vej: Danske virksomheder trækker den, <https://www.version2.dk/artikel/skrappe-persondata-regler-paa-vej-danske-virksomheder-traekker-den-793922>

GlobalSeur, Persondataforordningen kommer – Hvad betyder den for din virksomhed? <https://globalseur.com/fokusomraader-2/eu-persondataforordning/>

Scroll, What happens when content design crashes into the General Data Protection Regulation (GDPR)? <http://www.scroll.co.uk/what-happens-when-content-design-crashes-into-the-general-data-protection-regulation-gdpr/>

DI, Nye regler vil chokere virksomheder, <https://di.dk/dibusiness/nyheder/pages/nye-regler-vil-chokere-virksomheder.aspx>

DI Digital, Persondataforordningen - Implementering i danske virksomheder, <https://digital.di.dk/SiteCollectionDocuments/Vejledninger/Persondataforordningen/Vejledning%20om%20persondataforordningen%20med%20bilag.pdf>

Danske IT Advokater, Undersøgelse om it-konflikter og persondataforordningen i private virksomheder, <http://itadvokater.dk/wp-content/uploads/2016/06/it-advokat-rapport-100616.pdf>

IDC, GDPR is more than a security issue: Think Governance