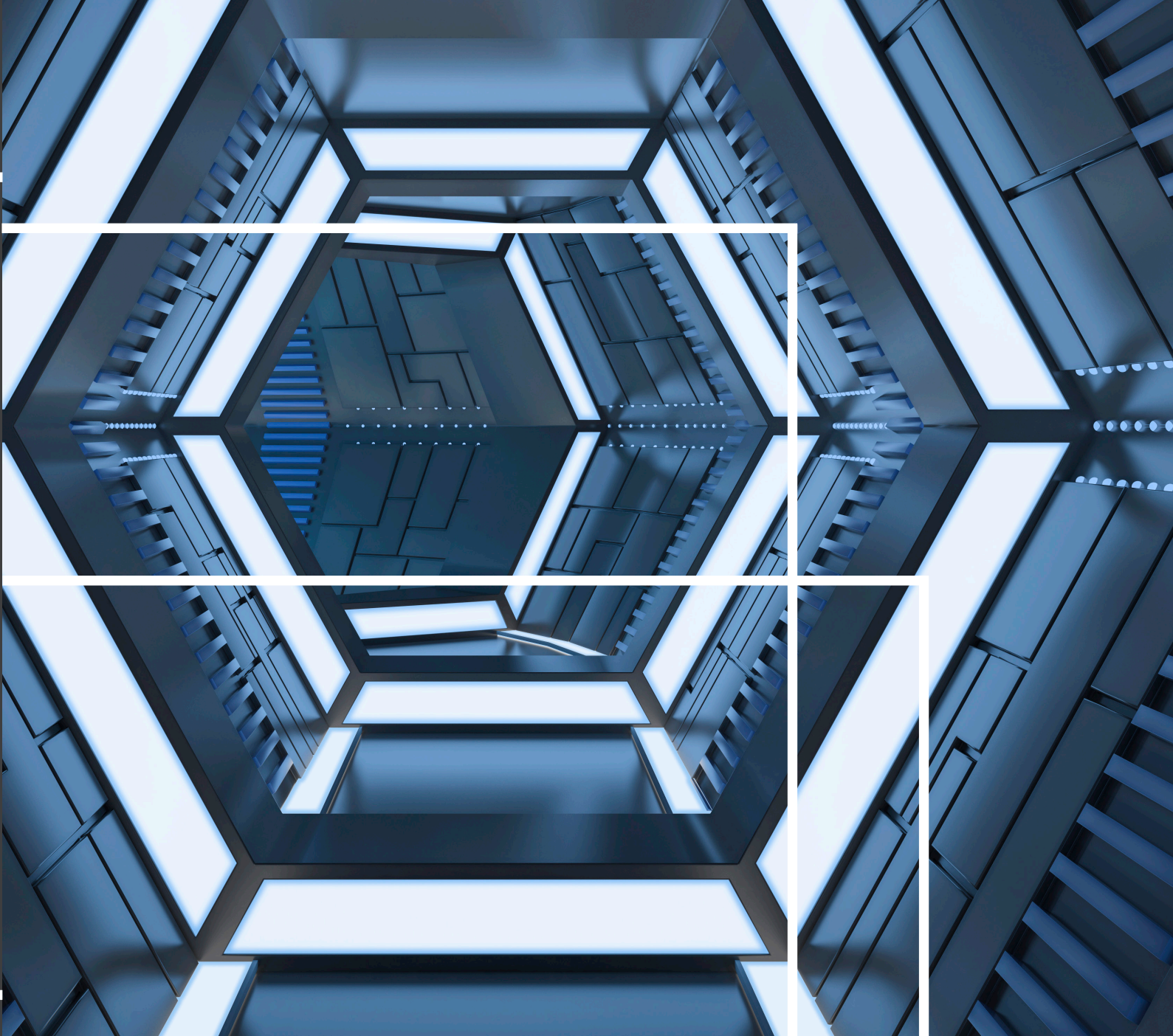




Compliance med persondataforordningen

Øget fokus på effektive GDPR-processer

Persondataforordningen skærper krav til behandling og beskyttelse af persondata, herunder dokumentationskrav, konsekvensanalyser, og en række nye rettigheder for de registrerede. Det kan blive dyrt ikke at have styr på de nye regler, og processen for at sikre fuld compliance kan være kompleks.

Er I sikre på, at I lever op til alle de organisatoriske og tekniske krav i forordningen – og kan I dokumentere det? Uanset hvor langt I er på GDPR-rejsen, kan vi hjælpe jer.

Persondataforordningen

Persondataforordningen gælder for al behandling af oplysninger om fysiske personer, som foretages af offentlige myndigheder, private virksomheder, foreninger mv. I praksis betyder det, at alle finansielle virksomheder uanset størrelse skal forholde sig til de nye regler. En overtrædelse af loven kan resultere i bøder på helt op til EUR 20.000.000 eller 4 % af virksomhedens samlede globale omsætning, hvis det beløb er højere.

Selvom forordningen byder på mange udfordringer i forbindelse med implementering og idriftsættelse, så kan de strenge krav også ende med at blive en gevinst for de finansielle virksomheder:

- Det bliver lettere for virksomheden at komme sig efter et brud på persondatasikkerheden, da det bliver lettere at fastslå, hvad der er sket, og hvad der skal gøres for at komme videre, når der er styr på processer, systemer og data.
- Virksomheden kan bruge pålidelighed, tillid og troværdighed som konkurrenceparametre i forhold til deres kunder.
- Virksomheden får skabt sig et overblik over, hvor den er mest eksponeret for skade, hvis personoplysninger ikke behandles korrekt.
- Virksomheden får et godt udgangspunkt for yderligere procesoptimeringer og eventuelle systemtilretninger.
- Virksomheden får ryddet op i persondata, får styrket datakvaliteten og får dannet sig et overblik, og det kan åbne op for en mere effektiv og proaktiv brug af eksempelvis kundedata.



Arbejdet med persondataforordningen er ofte meget krævende, også fordi der ikke er en klar praksis endnu. Det kan være en stor fordel at lade eksterne eksperter, som har erfaring fra andre projekter og opgaver med persondataforordningen, indgå i et samarbejde med virksomheden.



Sådan kan vi hjælpe

I PwC's Financial Services har vi et team af dedikerede medarbejdere bestående af jurister, projektledere, risikoeksperter og procesarkitektureksperter, der er specialiseret i persondataret.

Vores team spænder bredt i erfaring og uddannelsesmæssig baggrund. Vi har på den baggrund sammensat en palet af ydelser, som kan hjælpe dig og din virksomhed.

Bistand til implementering

Vi kan med afsæt i vores praktiske analyse- og implementeringserfaring komme med konkrete anbefalinger til en effektiv tilgang til optimal implementering og forankring og dermed hjælpe din virksomhed med at komme helt i mål. Vi kan bl.a.:

- assistere i programledelsen og i projektsporene
- udarbejde gap-analyser
- fastlægge risici ved behandling af personoplysninger og udarbejde konsekvensanalyser
- rådgive om processer, politikker, krav til interne kontroller, IT-sikkerhed samt vurderinger af teknologianvendelse i forhold til kravene i persondataforordningen
- bistå med udarbejdelse af databehandleraftaler
- bistå med implementeringen internt i virksomheden i relation til medarbejderne
- supportere med implementering af nye processer, teknologiske løsninger og uddannelse af medarbejdere
- supportere den egentlige idriftsættelse
- skabe en bedre kundeoplevelse.

Proceskortlægning og -design

I forhold til GDPR er det nødvendigt at dokumentere, hvilke persondata man opbevarer, i hvilke behandlinger dataene benyttes (processer), og hvilke personer der har adgang til dataene og gennemfører behandlinger. Vi kan hjælpe med at kortlægge og eventuelt optimere organisationens processer. En kortlægning indbefatter, at relationerne mellem persondata, behandlingsaktiviteter, systemer og roller bliver dokumenteret, hvilket bl.a. er nødvendigt for at kunne sikre, at man har lovlig behandlingshjemmel.

Desuden kan vi udvikle og implementere GDPR-specifikke best practice-processer, såsom håndtering af indsigtsbegæring, berigtigelser, tilsynsbesøg med mere.



Tilsynet stiller høje krav til IT-sikkerhed og overblik
over systemer og forventer en
velfungerende fordeling af roller og
ansvar på området.

IT-governance

Kravene fra GDPR rækker ind i både jeres forretningsområder og i IT. Langt de fleste forretningsprocesser understøttes på den ene eller anden måde af IT, og her skal man sikre en lang række af ting for at kunne leve op til GDPR. Det kræver en god governance omkring alle områder i IT, og at governance er kendt og forankret.

Vi kan hjælpe med at reviewe jeres nuværende IT-governance og komme med anbefalinger, så I kan sikre, at I bliver GDPR-compliant på dette område.

Har I ikke en IT-governance funktion eller opsætning, så kan vi hjælpe med at få implementeret en god governance, der er tilpasset jeres specifikke virksomhed, situation og baseret på best practice. Ligeledes kan vi tilbyde IT-governance assistance ved fx løbende at bistå jer med opfølgning og sparring.

GDPR-reviews

I forlængelse af implementeringen af persondataforordningen kan det være en god idé at få en uafhængig vurdering af, om forordningen er implementeret korrekt, og om den efterleves af medarbejderne.

Vi kan bl.a.:

- foretage review af organisations-, data-, proces- og systemarkitekturen for at fastlægge, om de styringsmæssige tiltag er implementeret korrekt i henhold til forordningen
- kontrollere at politikker og forretningsgange er indarbejdet i det daglige arbejde, og at der sker en efterlevelse af de registreredes rettigheder, som fx sletning og indsigt
- foretage review af IT-sikkerheden og teknologianvendelsen i forhold til forordningens krav
- give indspil til løsninger, som understøtter en god kundeoplevelse.

Fordelen ved et GDPR-review er bl.a., at:

- virksomheden får kortlagt og beskrevet de områder, hvor virksomheden ikke lever fuldt ud op til de nye krav
- virksomheden får lagt en handlingsplan (inklusive tidsplan) for, hvordan manglerne kan udbedres
- virksomheden får identificeret eventuelle optimeringsmuligheder i forhold til de løsninger, der anvendes.

Et GDPR-review kan naturligvis tilpasses virksomhedens konkrete ønsker.

Når Datatilsynet kommer

Datatilsynet foretager hvert år et antal planlagte tilsyn. Herudover foretager de også en række ad hoc-tilsyn som følge af konkrete hændelser.

Hvis din virksomhed bliver genstand for et tilsynsbesøg, kan vi hurtigt, effektivt og med kort varsel gennemføre et risikobaseret "light" GDPR-review for at afdække, om virksomheden efterlever persondataforordningen, eller om der er behov for hurtige udbedringer. Vi minimerer på den måde risikoen for, at din virksomhed bliver mødt med sanktioner fra Datatilsynet. Vi vil således – som led i denne proces – bidrage med at vurdere, om der er mulighed for at indføre såkaldte quick fixes, fx midlertidige ændringer i arbejdsrutiner for at kompensere for eventuelle mangler.

Vi kan også agere som bisidder under selve tilsynsbesøget.

Når Datatilsynet har været der

Datatilsynet har en række korrigerende beføjelser, hvis virksomhederne ikke efterlever persondataforordningen. Hvis Datatilsynet vælger at udtale kritik, udstede påbud eller i værste fald at sanktionere en overtrædelse med bøde, kan vi give konkrete og praktiske input til, hvor fokus skal sættes ind og bistå med udførelsen heraf.



“

Databeskyttelsesrådgiverens rolle skal afgrænses korrekt i forhold til fx compliance, risikostyring og GDPR-drift for at leve op til myndighedernes forventninger.

Revisionserklæringer

PwC oplever en stigende efterspørgsel på revisionserklæringer. Det er en proces, der normalt foretages årligt, og der findes som udgangspunkt to varianter:

- en general erklæring, som forholder sig til virksomhedens persondatakontroller
- en specifik erklæring, som fokuserer på netop databehandleraftalen til en specifik kunde/samarbejdspartner.

GDPR Analytics

PwC's værktøj, GDPR Analytics, kan opdage og klassificere personoplysninger i såvel strukturerede data (IT-systemer) som ustrukturerede data (e-mails, fildrev). GDPR Analytics kan monitorere på tværs af virksomheden og virksomhedens eventuelle andre juridiske enheder.

Det betyder bl.a., at din virksomhed kan finde ud af, om oplysninger om den samme kunde er registreret i mere end et system, og om det er de samme oplysninger, og hvorvidt personfølsomme oplysninger er tilstrækkeligt adgangsbegrænsede.

GDPR Analytics er udviklet baseret på AI-teknologi (artificial intelligence) og vil derfor hele tiden kunne øge sin performance.

DPO – Compliance og service

En databeskyttelsesrådgiver (DPO) er en rådgiverfunktion, der skal inddrages i alle spørgsmål om databeskyttelse og rådgive om de databeskyttelsesretlige regler. Mange af de store finansielle institutioner har valgt at ansætte en DPO. Da funktionen er en nyskabelse i persondatalovgivningen, ser vi dog, at mange virksomheder har udfordringer med at definere DPO'ens rolle og ansvar. Vi kan komme med konkrete anbefalinger til, hvordan DPO-funktionen bør opbygges og idriftsættes og dermed sikre en korrekt forståelse af DPO'ens ansvarsområde. Vi kan bl.a. bistå med udarbejdelsen af skriftlige procedurer, hvori databeskyttelsesrådgiverens involvering, virke og rapportering er beskrevet.

Vores team bistår også gerne med midlertidig varetagelse af DPO-rollen i forbindelse med ferie, orlov mv. På den måde sikres et konstant kontaktpunkt i virksomheden samt rettidig indberetning af eventuelle databrud, selv når DPO'en er fraværende.

Vil du vide mere?

Har du spørgsmål – eller har du brug for konkret rådgivning inden for persondatalovgivningen – så er du altid velkommen til at kontakte vores team, der er specialister inden for persondata i den finansielle sektor.

Vores GDPR-ydelser til den finansielle sektor er forankret i teamet Risk & Compliance, som med afsæt i en operationel tilgang tilbyder ydelser som governance, organisering, processer og data, hvor effektivitet, transparens og vidensdeling er nøgleord. Vi er et stærkt team af bl.a. jurister, risikoeksperter og procesarkitekter.



Janus Mens

Partner, Risk & Compliance

M: 2262 0759

E: janus.mens@pwc.com



Helle Dreyer

Director, Operationel Risikostyring & Compliance

M: 6155 5181

E: helle.dreyer@pwc.com