GDPR GUIDE

☑ **Forstå reglerne på 10 minutter**

☑ **7 trin til at blive compliant**

☑ **GDPR tjekliste**

WTC advokaterne

Velkommen til GDPR guide

Vi har lavet denne e-bog som inspiration til dig og din virksomheds GDPR-arbejde. Guiden er interaktiv, så hvis du læser den på en skærm, har du mulighed for at klikke på links for at få mere viden og på video ikonet for at se en video om emnet. Du kan også afkrydse felterne i tjeklisten på side 11 blot ved at klikke i dem med din mus.

God fornøjelse.

Indhold

7 trin til at blive compliant.....3

Fortegnelse 4

Risikoanalyse.....5

Den interne datapolitik.....6

Den eksterne datapolitik 7

Samtykke 8

Databehandleraftale.....9

Undervisning 10

GDPR compliant tjekliste 11

GDPR ordbog.....12

Kontaktinformation på WTC advokaterne.....13

7 trin til at blive compliant

DATATILSYNET STØDER JÆVNLIGT PÅ GDPR FORSEELSER. DET KAN KOSTE VIRKSOMHEDER DYRT, SÅ SØRG FOR AT HAVE STYR PÅ REGLER OG PROCEDURER, INDEN DATATILSYNET KOMMER PÅ BESØG HOS DIG!

De fleste har i dag hørt om GDPR, der er EU's regelsæt lavet for at beskytte privatpersoners persondata og retten til privatlivets fred.

Vejen til at blive compliant som virksomhed er individuel, og der findes ikke en standard løsning, der passer alle. Det er derfor nødvendigt, at du sætter dig ind i din virksomheds individuelle situation og overvejer, om der bør indarbejdes særlige tiltag. Denne guide kan ikke erstatte juridisk rådgivning, men det er dog vores oplevelse, at compliancearbejdet typisk kan deles op i de 7 "trin" nedenfor.

Trin-for-trin guide til at blive compliant

1. Fortegnelse
2. Risikoanalyse
3. Den interne datapolitik
4. Den eksterne datapolitik
5. Samtykke
6. Databehandleraftaler
7. Undervisning

1. Fortegnelse

Det første du skal gøre er at kortlægge, hvilke data virksomheden har, og hvor oplysningerne er opbevaret. Dette gør du ved at lave en såkaldt fortegnelse, også kaldet en "data mapping", hvor du registrerer alle de persondata, som virksomheden opbevarer.

Fortegnelsen har det overordnede formål at give overblik over virksomhedens behandling af personoplysninger. Samtidig er den med til at danne grundlag, for at kunne dokumentere de behandlingsaktiviteter, der forekommer i virksomheden, hvis Datatilsynet melder deres ankomst.

Det er vores erfaring, at en grundigt udarbejdet fortegnelse danner det bedste udgangspunkt for det videre compliancearbejde.

Vi anbefaler derfor, at du investerer tid og energi i at undersøge og besvare følgende punkter i fortegnelsen. Dette gør virksomhedens videre arbejde lettere og mere overskueligt.

Fortegnelsen skal som minimum indeholde oplysninger om:

- Hvem virksomheden behandler personoplysninger om.
- Hvilke personoplysninger virksomheden har.
- Hvor virksomheden opbevarer personoplysningerne.
- Formålet med virksomhedens behandling.
- Lovgrundlaget for behandlingen.
- Hvor personoplysningerne kommer fra.
- Den forventede opbevaringstid.
- Hvem personoplysningerne videregives til, herunder hvilke kategorier af personoplysninger-der videregives til de forskellige modtagere.

Vi anbefaler, at du opstiller fortegnelsen i et Excel ark, da Excel er et simpelt og universalt værktøj, som er velegnet til at danne et overblik. Der findes også andre digitale løsninger på markedet, der kan hjælpe dig med at udarbejde en fortegnelse – typisk mod betaling.

Når du har fået overblik over virksomhedens persondata, er du klar til at gå videre til det næste trin.

2. Risikoanalyse

Når de forskellige persondata er kortlagt i fortegnelsen (data mapping), skal der udfærdiges en risikoanalyse.

Du skal nu udfærdige en risikoanalyse for virksomhedens behandling af personoplysninger – er der en lav, mellem eller høj risiko for et databrud ved virksomhedens behandling af personoplysningerne? Analysen tager udgangspunkt i fortegnelsen fra det første trin, og analysen bør udarbejdes i dialog med virksomhedens IT-afdeling/ IT-person.

Risikoanalysen er et værktøj, som du skal bruge, når du skal udarbejde de interne tekniske og organisatoriske politikker, som skal være gældende i virksomheden. Med andre ord – du skal kende de risici og IT-svagheder virksomheden har, før du kan indføre tiltag, der mindsker risikoen for databrud.

Start med at foretage en kortlægning af risikoen for de registreredes rettigheder. En sådan risiko kan eksempelvis være identitetstyveri eller tab af ære og velfærd - men rettighederne dækker meget bredt. Et eksempel på de forholdsregler man kan tage, for at minimere disse risici er, at kryptere virksomhedens kommunikation eller indføre kontroller der sikrer, at e-mails kun sendes til den tilsigtede modtager.

Derefter skal du foretage en risikoanalyse af de databehandlere, som behandler personoplysninger for dig. Dette gøres med henblik på at vurdere, om det er sikkert, at persondata videregives til databehandleren samt for at klarlægge, hvor omfattende kontrollen af databehandleren skal være.

3. Den interne datapolitik

Den interne datapolitik er det regelsæt, som virksomheden og alle medarbejderne forpligter sig til at følge, når virksomheden behandler personoplysninger.

EN PRAKTISK MÅDE AT GRIBE PROCESSEN AN PÅ ER VED AT TÆNKE I SCENARIER, DVS. ALLE DE SITUATIONER, SOM MAN KAN KOMME I TANKE OM, HVOR PERSONDATA KOMMER IND I VIRKSOMHEDEN.

Det betyder i praksis, at virksomheden skal lave et regelsæt for behandlingen af personoplysninger i virksomheden. Regelsættet skal udleveres til alle virksomhedens medarbejdere. Den interne datapolitik skal indeholde en beskrivelse af virksomhedens tekniske og organisatoriske regler, så medarbejderne kender til procedurer indenfor behandling af persondata men også til reglerne, hvis der sker sikkerhedsbrud.

Interne datapolitikker kan variere fra virksomhed til virksomhed, og du skal derfor altid lave en individuel vurdering af, om de løsninger du har indarbejdet i virksomhedens interne datapolitik er tilstrækkelige til at opfylde forordningens krav.

Lav klare retningslinjer for egenkontrol, så du jævnligt sikrer, at de opsatte regler og processer også bliver ført ud i livet. Får du eksempelvis slettet data rettidigt, opdateret dokumenter løbende, og har du den fornødne sikkerhed på plads?

4. Den eksterne datapolitik

Hvis oplysninger om en person indsamles, skal der udleveres en række oplysninger om bl.a. virksomhedens kontaktoplysninger, formålene med indsamlingen, den registrerede persons rettigheder, modtagerne af oplysningerne, klageadgang m.v.

TAG UDGANGSPUNKT I JERES FORTEGNELSE, NÅR I UDFÆRDIGER DEN EKSTERNE DATAPOLITIK

Datapolitikken skal skrives i et lettilgængeligt sprog, som virksomheden skal udlevere til de personer, som virksomheden behandler oplysninger om.

Ofte er der behov for at udarbejde flere forskellige datapolitikker, da datapolitikkens indhold vil variere afhængigt af, hvem virksomheden behandler oplysninger om (er det medarbejdere, kunder, samarbejdspartnere eller andre?), og til hvilket formål behandlingen sker.

5. Samtykke

Det er ikke alle typer persondata, virksomheden må behandle uden at spørge den registrerede om lov først. Dette er typisk tilfældet, hvis virksomheden behandler "følsomme personoplysninger".

Du bør allerede have taget stilling til, om virksomheden behandler følsomme personoplysninger i fortegnelsen fra det første trin. Du bør også i første trin have undersøgt virksomhedens lovgrundlag for behandlingen. Hvis virksomheden ikke har et lovgrundlag for behandlingen, må virksomheden bede den registrerede om et samtykke, hvis behandlingen i øvrigt findes saglig og nødvendig.

Derudover skal der i de fleste tilfælde udfærdiges en samtykkeerklæring til virksomhedens medarbejdere, hvis virksomheden bruger billeder af medarbejdere til markedsføring på internettet - eksempelvis på virksomhedens hjemmeside.

Det er meget vigtigt, at samtykket udformes korrekt, da det ellers ikke er gyldigt. Derfor anbefaler vi, at samtykket udfærdiges af en advokat.

6. Databehandleraftaler

1

Virksomheden skal have en databehandleraftale med de samarbejdspartnere, som virksomheden overfører persondata til. Det kan f.eks. være virksomhedens lønbureau eller det firma, der opbevarer eller laver backup af virksomhedens data.

2

Skal der udfærdiges nye databehandleraftaler, er det vigtigt, at de opfylder kravene i forordningen samt tager højde for, om virksomheden er dataansvarlig eller databehandler. En databehandleraftale er en bindende kontrakt, som skal være skriftlig og skal opbevares elektronisk.

3

Derudover skal sikkerheden være tilstrækkelig beskrevet, hvorfor det i mange tilfælde er nødvendigt, at der udfærdiges et bilag til aftalen om de tekniske krav til databehandleren, hvilket et IT-sikkerhedsfirma kan være behjælpelig med.

4

Som dataansvarlig skal du ligeledes kontrollere dine databehandlere. Dette skal typisk ske én gang om året, men afhænger bl.a. af mængden af persondata, databehandleren behandler for dig samt følsomheden heraf.

5

En kontrol af en databehandler vil typisk bestå i indhentelse og gennemgang af en ISAE3000 eller lignende erklæring, et fysisk kontrolbesøg hos databehandleren eller kontrol via en række spørgsmål til databehandleren samt indhentelse af dokumentation.

6

Databehandleraftalen skal indeholde instruks til databehandleren om, hvordan oplysningerne skal behandles. Du kan altså ikke nøjes med at henvise til "hovedaftalen" eller lignende dokumenter.

7. Undervisning

Som virksomhed har I pligt til løbende at undervise og træne jeres medarbejdere i databeskyttelsesforordningen (GDPR) og IT-sikkerhed. I skal bl.a. sikre jer, at medarbejderne forstår vigtigheden af, at jeres fastlagte politikker og procedurer på området overholdes. Det er altså ikke nok at have procedurer mv. på plads. Det er først, når medarbejderne trænes i og forstår, hvordan de skal agere i hverdagen for at overholde procedurerne, at virksomheden er compliant.

Der ligger et stort arbejde i at leve op til databeskyttelsesforordningen, især fordi det handler om at ændre medarbejdernes adfærd. Det er svært! Derfor skal medarbejderne trænes. Det er ligeledes vigtigt at undervise medarbejderne i IT-sikkerhed.

Jeres medarbejdere er det største aktiv men også det svageste led, når det handler om jeres IT-sikkerhed. Faktisk starter 9 ud af 10 sikkerhedsbrud hos medarbejderne.

Hvis I vælger at få en advokat og en IT-sikkerhedsekspert til at stå for undervisning og træning, sikrer I jer, at både de juridiske og sikkerhedsmæssige forhold bliver formidlet korrekt til jeres medarbejdere.

Vil du læse mere om, hvordan WTC kan hjælpe med træning af jeres medarbejdere i databeskyttelsesforordningen (GDPR) og IT-sikkerhed, så læs mere på vores hjemmeside.

GDPR compliance tjekliste

Læser du guiden på din skærm, kan du afkrydse felterne, blot ved at klikke i dem med din mus.

☑ **Læs GDPR guide**
Tillykke, du er nu igennem guiden og klar til at tjekke, om din virksomhed overholder persondataforordningen.

☐ **Lav en fortegnelse/data mapping**
Kortlæg, hvilke persondata virksomheden har, og hvor oplysningerne er opbevaret.

☐ **Risikoanalyse**
Udfærdig en risikoanalyse for virksomhedens behandling af personoplysninger.

☐ **Den interne datapolitik**
Lav et regelsæt for behandlingen af personoplysninger i virksomheden, og udlevér den til virksomhedens medarbejdere.

☐ **Den eksterne datapolitik**
Lav en ekstern datapolitik, og placér den synligt på jeres hjemmeside.

☐ **Samtykke**
Indhent samtykke fra medarbejdere og kunder, hvis din virksomhed indhenter personfølsomme oplysninger om dem.

☐ **Databehandleraftaler**
Gennemgå eksisterende databehandleraftaler og opret nye, hvis nødvendigt. Indsæt i din kalender, at du mindst én gang årligt skal kontrollere dine databehandlere.

☐ **Undervisning**
Arrangér undervisning og træning til alle medarbejdere inden for databeskyttelses-forordningen (GDPR) og IT-sikkerhed, eller bestil undervisning og træning fra et eksternt firma, hvis du ikke selv vil stå for undervisningen.

GDPR ordbog

Dataansvarlig
En virksomhed, myndighed eller organisation der behandler persondata.

Databehandler
En virksomhed, myndighed eller organisation der behandler persondata på vegne af den dataansvarlige.

Dataansvarlig
Den dataansvarlige afgør hvorfor (med hvilket formål) og hvordan (med hvilke hjælpemidler), personoplysningerne behandles. Som udgangspunkt er alle virksomheder dataansvarlige, da de ligger inde med både persondata på medarbejderne samt kundedata.

Databrud
En hændelse der medfører tilintetgørelse, tab, ændring, uautoriseret adgang eller uautoriseret videregivelse af de personoplysninger, man behandler.

Datatilsynet
Den myndighed der fører tilsyn med, at Databeskyttelsesforordningen overholdes.

Databehandleraftale
En aftale der indgås mellem databehandler og dataansvarlig for at sikre, at persondata beskyttes og behandles korrekt.

Compliant
At være Compliant betyder, at du som virksomhed har fastlagt nogle processer og retningslinjer for at sikre, at du overholder de krav og regulativer, der findes.

Følsomme personoplysninger
Helbredsoplysninger, fagforeningsmæssige tilhørsforhold, race, etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, genetiske data, biometriske data, seksuelle forhold eller seksuel orientering.

Persondata
Alle data der kan henføres til bestemte personer f.eks. navn, e-mailadresse, telefonnummer etc.

Registrerede
Den eller de personer som persondataene omhandler. De registrerede ejer de data, der vedrører dem.

Samtykke
Den registrerede kan give tilsagn om noget gennem samtykke, f.eks. at man godkender, at der sker en behandling af vedkommendes personoplysninger.

Vi kan hjælpe

Det ikke er nemt hverken at forstå eller arbejde med persondataforordningen.

WTC advokaterne har specialiseret sig i persondatalovgivningen og har hjulpet mange, både store og små virksomheder, med at få helt styr på persondataforordningen.

Vi tager også gerne hånd om din virksomheds compliance arbejde.

Kontakt os gerne for en uforpligtende samtale.

Gabriel L. Martiny
Advokat (H) | Partner

M glm@wtc.dk
T +45 48 22 00 40
D +45 48 22 00 13

Indholdet i denne guide er ikke ment som og kan ikke erstatte juridisk rådgivning.

WTC advokaterne