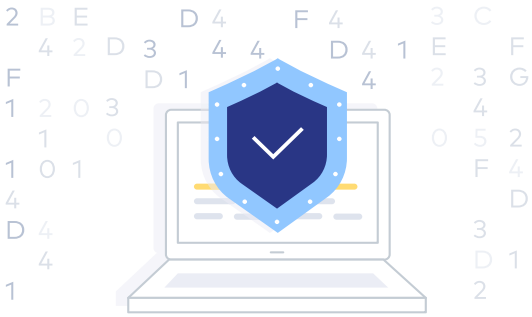
Sådan forbereder du dig til GDPR

Der har været en masse snak om en ny lovgivning, der kommer op i EU. Den generelle databeskyttelsesforordning eller GDPR er en ny lov, der regulerer, **hvordan europæiske borgeres data skal håndteres, uanset nationaliteten af den organisation, der håndterer dataene.**

GDPR fastsætter meget specifikke retningslinjer for erhvervelse, forvaltning og anvendelse af data, der enten er bundet til nogen hjemmehørende i EU eller indsamlet af et selskab, der opererer i EU. Manglende overholdelse af denne nye lov kan betyde store bøder.

Dette whitepaper vil hjælpe dig med at forstå den nye lov og hvad den betyder for den måde, hvorpå din organisation indsamler, opbevarer og bruger data. Det dækker nogle af de juridiske definitioner omkring GDPR, indeholder værktøjer til evaluering af, om din organisation er kompatibel med GDPR, og foreslår de næste trin for virksomheder, der skal overholde loven.



FFW

Kontakt FFW

For at forberede til GDPR, er det vigtigt at forstå, hvilke data du opretter, hvor og hvordan du behandler og gemmer dem, og hvordan din organisation kan understøtte brugernes rettigheder i dine systemer.

Har du brug for hjælp til nogle af trinene i at overholde de nye regler, så kontakt FFW. Vi leverer løsninger til at hjælpe organisationer af alle størrelser og slags med at forberede deres datasystemer til GDPR.

Lær mere på:

ffwagency.com facebook twitter linked in

Hvad er GDPR?

I 2016 godkendte EU sin generelle databeskyttelsesforordning (GDPR) for at beskytte europæiske borgeres data.

Loven er designet til at sikre **"beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri bevægelighed for sådanne data".**

Men hvad betyder det?

Kort fortalt er GDPR en ny lov, som beskytter dataene fra Europas befolkning. Der er to typer lovgivning i EU:

Direktiver,
hvor medlemsstaternes parlamenter skal passere lovgivningen

Forordninger,
som straks finder anvendelse i medlemslandene

GDPR er en forordning, hvilket betyder, at det fra den tid, det gælder som lov, er det en lov i hver enkelt EU-medlemsstat. Men da loven er fokuseret på databeskyttelse, gælder den for enhver organisation, der samler, opbevarer eller udnytter data fra en EU-borger, selvom organisationen er baseret uden for EU.

Når du læser om GDPR, kan du støde på sætningen **"Regler for beskyttelse af fysiske personer med hensyn til behandling af personoplysninger".** Dette er en vigtig sætning, da det indeholder flere juridiske sondringer, som organisationer skal tage hensyn til:

En fysisk person er et levende individ

Personoplysninger er oplysninger om en identificeret eller identificerbar fysisk person. Dette kan være et:

- Navn
- Identifikationsnummer
- Lokaliseringsdata
- En online identifikator eller enhver anden faktor
- Der er specifik for den fysiske persons fysiologiske, genetiske, mentale, økonomiske, kulturelle eller sociale identitet

Behandling betyder enhver handling eller et sæt af handlinger, der udføres med personoplysninger. Dette omfatter:

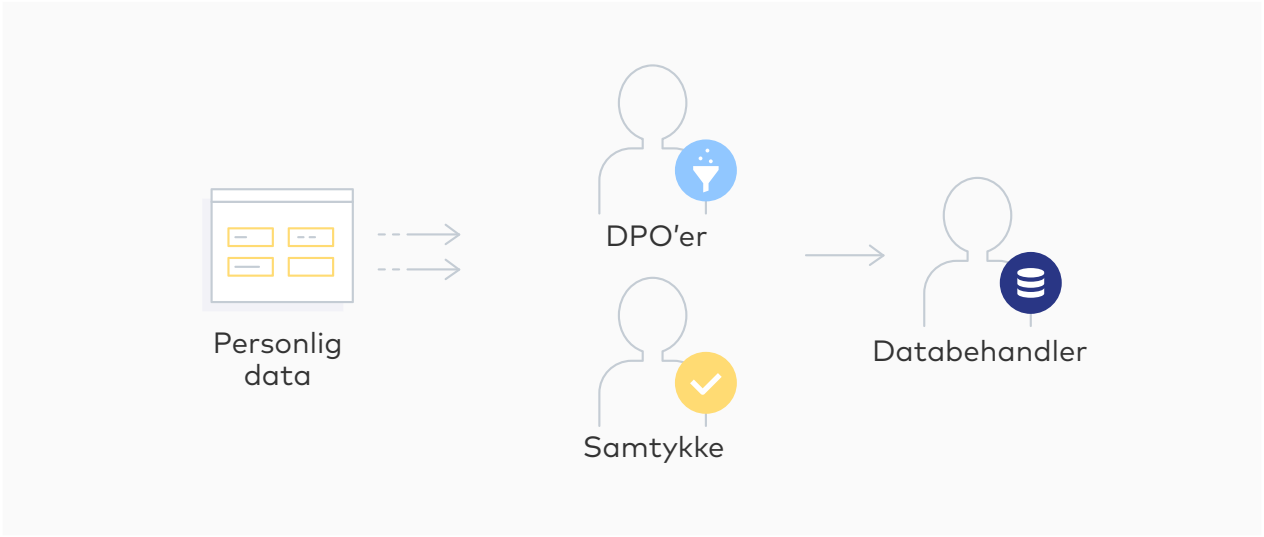
- Indsamling
- Registrering
- Organisering
- Opbevaring
- Tilpasning eller ændring
- Indhentning
- Konsultation
- Brug
- Videregivelse ved transmission
- Formidling eller på anden måde tilgængeliggørelse og sletning eller destruktion af disse data.

At forstå omfanget af "personlige data" og "behandling" kan hjælpe organisationer med at få en bedre forståelse for, hvor massiv denne lov er. **Forordningen træder i kraft den 25. maj 2018.**

Før det sker, skal organisationer sikre sig, at de er fuldt kompatible. For virksomheder, der oplever overtrædelser, der resulterer i tab af personlige data (såsom virksomheden Talk Talk, der mistede 170.000 personers data), vil bøderne være smerteligt høje. **Lavtakst bøder er 10 mio. € , eller 2% af den årlige omsætning,** alt efter hvad der er højest. For højtakst bøder er disse tal det dobbelte.

Hvem skal overholde GDPR?

Kort fortalt: alle. Hvis der blot er en chance for, at din organisation har data fra en EU-borger et eller andet sted i dine systemer, bør du sørge for, at du er i overensstemmelse med den nye lov. Derudover er der nogle få vigtige definitioner at forstå, når man forbereder sig til GDPR-overholdelse.



DPO'er (Data Protection Officer)

DPO'eren er den organisation eller det individ, der er "ansvarlig" for dataene. Officielt fastlægger en DPO'er formål og midler til behandling af personoplysninger.

En DPO'er kan være en fysisk eller juridisk person, offentlig myndighed, agentur eller et andet organ, der kan handle alene eller i fællesskab med andre.

For eksempel gav du os dit navn, din e-mail og muligvis nogle oplysninger om din arbejdsgiver, da du downloadede dette whitepaper fra FFW. Det gør os til DPO'er for de data, vi indsamlede fra dig, da du udfyldte downloadformularen på vores hjemmeside.

Samtykke

DPO'eren er ansvarlig for at behandle data lovligt, retfærdigt og på en transparent måde. DPO'ere kan udvise lovlighed, hvis en registreret har givet samtykke til behandlingen af hans eller hendes personlige data. Samtykke skal gives af egen fri vilje og skal give en specifik, informeret og entydig angivelse af den registreredes ønsker.

Loven er her meget klar omkring, hvad der udgør et samtykke; brugere skal afgive en erklæring eller udføre en klar, bekræftende handling med angivelse af, at deres data kan anvendes.

Retningslinjerne for samtykke betyder, at der skal være en klar fortrolighedserklæring til brugere, når de indtaster deres data. Bekendtgørelsen skal klart angive, hvorfor der spørges efter samtykke, og hvad der skal ske med disse data - derfor skal folk altid tilmelde sig, snarere end at framelde sig. Smarte ord og forudfyldte afkrydsningsfelter vil blive betragtet i strid med samtykkereglerne. Som DPO'er skal det være klart, at du beder om tilladelse til at bruge dine besøgendes data, og hvad det betyder, hvis du beder om det.

Databehandler

Databehandleren er den organisation eller person, der manipulerer, gemmer eller destruerer dataene. Akkurat som med en DPO'er kan en databehandler være en fysisk eller juridisk person, offentlig myndighed, agentur eller et andet organ.

En databehandler kan faktisk manipulere oplysninger på DPO'erens vegne.

Et andet eksempel på dette er, at nogle af de services, vi tilbyder hos FFW, omfatter opbevaring og indhentning af vores kunders data på deres egne kunder. Det gør os til en databehandler for andre parter, selvom vi ikke udfører nogle databehandlinger af dataene for vores egen organisatoriske fordel.

GDPR handler om beskyttelse og privatliv

GDPR er meget eksplicit omkring, at organisationer skal være i stand til og klar til at påvise overholdelse af lovens krav. Målet her er at være proaktiv, ikke reaktiv; Hvis nogen kontakter dig for at sikre sig, at du overholder GDPR, bør du være i stand til at påvise, at din organisation følger de seks principper for GDPR.

Ifølge GDPR, skal alle data...

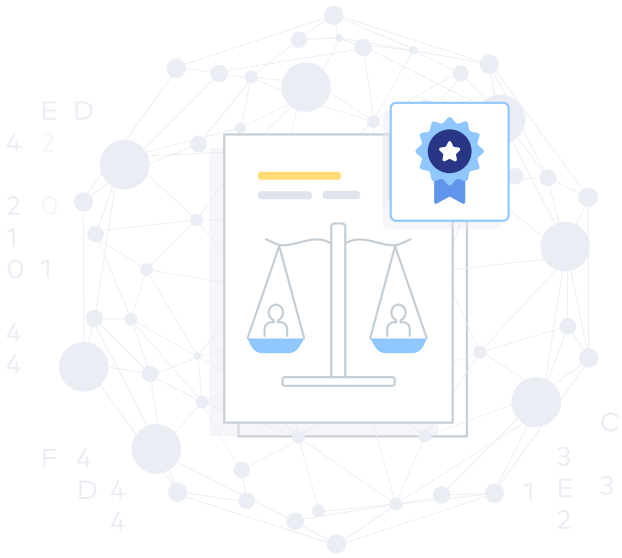
1. Behandles lovligt, retfærdigt og på en transparent måde
2. Indsamles for specificerede, eksplicitte og legitime formål
3. Holdes ajour
4. Begrænses til, hvad der er nødvendigt
5. Ikke tillade identifikation af personer i længere tid end nødvendigt
6. Behandles på en måde, der sikrer en passende sikkerhed

Når de oversættes, kan disse principper koges ned til følgende idé:

Data skal indsamles med udtrykkeligt samtykke, og alle brugere skal vide præcis, hvad deres data vil blive brugt til. Dataindsamling og opbevaring bør begrænses til, hvad din organisation absolut har brug for at vide om en bruger. Din organisation skal kunne dokumentere, at en anmodning om samtykke blev præsenteret tydeligt, og at disse data ikke sælges, ændres eller på anden måde misbruges. Systemer bør ikke stole på forældede eller flere år gamle data til markedsføringsformål, og hvis brugere ønsker at opdatere deres data eller inddrage deres samtykke, skal de være i stand til nemt kunne gøre det.

Frem for alt skal dataene opbevares et sikkert sted og behandles på en måde, der sikrer de personer, som dataene tilhører.

Forstå dine brugeres rettigheder



GDPR-reglerne blev udformet omkring europæiske borgeres rettigheder med hensyn til deres person-oplysninger. Disse er:

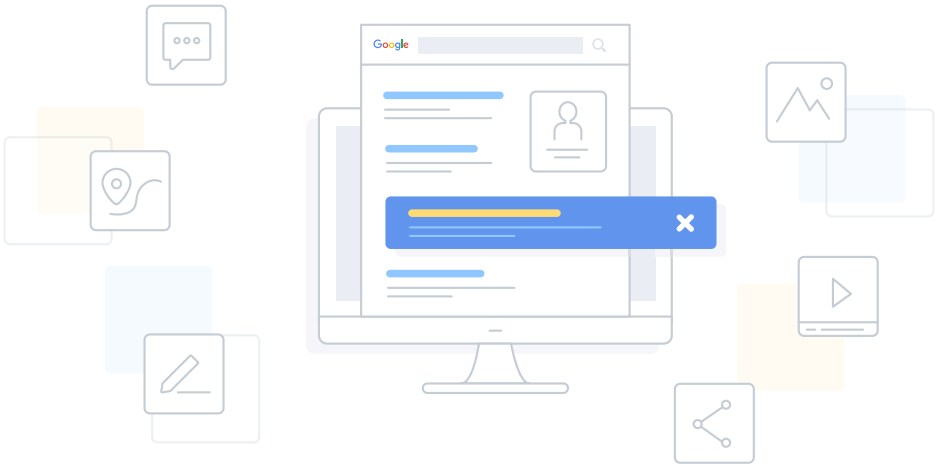
- Retten til at blive informeret
- Retten til adgang
- Retten til at korrigere
- Retten til at slette (ret til at blive glemt)
- Retten til at begrænse behandling
- Retten til dataportabilitet
- Retten til at gøre indsigelse
- Retten til ikke at blive underlagt automatiseret beslutningstagning, herunder profilering

Udover at sikre, at din organisation følger reglerne om at indsamle, opbevare og manipulere data sikkert, skal du også sørge for, at du har systemer, der giver de europæiske borgere mulighed for at udøve deres rettigheder med hensyn til deres data. **Du bør sørge for, at du har processer, procedurer og træning i dit team, så brugerne kan udøve deres rettigheder.**

Desuden skal alle former for kommunikation være i en kortfattet og let tilgængelig form. Brug klart og almindeligt sprog, selv i juridiske dokumenter - det kan være nødvendigt at få disse revideret, så de er mere tilgængelige for offentligheden.

Et eksempel på at opbygge en ramme for datarettigheder

For et eksempel på, hvordan du sikrer, at dit system er kompatibelt, behøver du ikke at kigge længere end til Google. I maj 2015 fastslog EU-Domstolen, at søgemaskinerne er ansvarlige for det indhold, de peger på, og derfor skal de overholde EU's privatlivslovgivning. Specielt blev Google bedt om at overholde retten til at blive glemt.



"Ifølge Reuters kan "Internet-virksomheder tvinges til at fjerne irrelevante eller for omfattende personlige oplysninger fra søgemaskinernes resultater ... Den Europæiske Unions Domstol opretholdt klagen fra en spansk mand, der protesterede mod, at Google søgninger på hans navn viste links til en avisartikel fra 1998 om beslaglæggelse af hans hjem. "Under denne dom bør enhver ikke-offentlig person" kunne fjerne deres digitale spor fra internettet".

For at overholde brugernes ret til at blive glemt, oprettede Google en ramme for at fjerne søgeresultater fra EU-indekset og etablerede en proces, hvor brugerne kunne anmode om, at deres oplysninger blev fjernet.

Dette er et klart eksempel på, hvordan en massiv organisation etablerede processer og procedurer for folk til at udøve deres rettigheder - og hvis nogen kan fjerne deres information fra Google, så bør de også kunne fjerne deres information fra dine systemer.

Gennemfør en 8-trins forberedelsesplan for GDPR

Det første skridt i forberedelsen til det nye GDPR er at evaluere dine eksisterende politikker og procedurer. Hvilke data indsamler du, og hvorfor? Er disse data sikre? Kan brugere fjerne deres data fra dine systemer? Etabler processer, procedurer og udfør personaletræning, så din organisation kan håndtere mennesker, der udøver deres rettigheder.

Derudover er der nogle få vigtige ting, du bør gøre for at forberede din organisation:

1. Skab bevidsthed

Sørg for, at beslutningstagere og nøglepersoner i din organisation er opmærksomme på, at loven ændrer sig til GDPR. De har brug for at anerkende den indflydelse dette sandsynligvis vil have, og du har brug for deres støtte for at foretage de nødvendige ændringer i dine systemer.

2. Gennemfør en information audit

Dokumentér hvilke personlige data du har, hvor de kommer fra, og hvem du deler dem med. Som en del af dette, skal du gennemgå dine nuværende oplysninger om beskyttelse af personlige oplysninger, og oprette en plan for at foretage de nødvendige ændringer. Tjek også hvilke procedurer du har på plads for at sikre, at europæiske borgere kan udøve deres rettigheder på dit website. Det bør være enkelt for brugerne at levere, opdatere eller slette deres personlige data fra din organisations systemer.

3. Indsæt en plan for håndtering af anmodninger om adgang

Hvis du får en anmodning om adgang fra en person eller fra en officiel organisation, der skal kontrollere, om du overholder loven, bør du have en plan på plads. Sørg for at oprette eller opdatere eventuelle procedurer, du har til at levere data, og planlæg, hvordan du håndterer disse anmodninger, hvis eller når de kommer ind.

4. Identificér lovligt grundlag for behandling

Forstå, hvordan du behandler data og af hvilke årsager, og sørg for, at dine brugere giver udtrykkeligt samtykke til disse handlinger. Før GDPR træder i kraft, skal du sørge for, at du behandler data lovligt, har dokumentation til støtte for det, og sørge for, at du har opdateret din persondatapolitik for at forklare det.

5. Tjek dit system for mindreårige

Dette er et meget vigtigt skridt og et, som nogle organisationer kan overse. Afhængigt af hvordan du indsamler data, kan du blive nødt til at sætte systemer på plads for at verificere enkeltpersoners alder og få tilladelse af forældre eller værger for børn, hvis data du muligvis indsamler.

6. Udform en plan for brud på datasikkerheden

Ingen organisation ønsker at få deres data kompromitteret. Ikke desto mindre skal du først sørge for, at dine data er så beskyttede som muligt, og for det andet, at du har procedurer og systemer til at registrere, rapportere og undersøge brud på personlige data.
For at sikre, at dine systemer er i overensstemmelse med beskyttelsesreglerne, skal du gøre dig fortrolig med den seneste vejledning fra Artikel 29-Gruppen vedrørende databeskyttelse. Kortlæg desuden, hvordan du vil implementere privatlivsimplikationsanalyse for din organisation.

7. DPO'er (Data protection officers)

Udpeg en person (inden for din organisation eller en juridisk enhed) til at tage ansvar for overholdelse af databeskyttelse. Afgør, hvor denne person vil befinde sig i organisationsstrukturen, og dokumentér, hvem din DPO'er er.

8. Forstå internationale retningslinjer

Hvis din organisation opererer i mere end en medlemsstat,

skal du afgøre, hvem der er din ledende tilsynsførende for databeskyttelse. Er du ikke sikker på, hvor du skal starte? I december 2016 offentliggjorde Artikel 29-gruppen sine **Retningslinjer for Identifikation af en Tilsynsmyndighed** for at hjælpe organisationer med denne afgørelse. For at gøre processen med at identificere en tilsynsmyndighed lettere, er det vigtigt at forstå, hvor din organisation træffer beslutninger vedrørende forarbejdning.

Udpege en repræsentant

Organisationer, der ikke er etableret i EU, men som opererer i EU, eller som behandler data fra personer, der bor i EU, skal finde en repræsentant i EU.

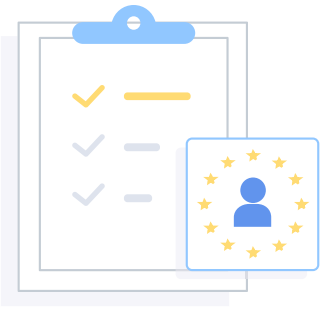
Ifølge GDPR-artikel 4 kan:
"Enhver fysisk eller juridisk person, der er bosat i en af medlemsstaterne, udpeges som repræsentant i Unionen for en ikke-EU-baseret virksomhed".

Det er repræsentantens ansvar at tilvejebringe de krævede oplysninger, der måtte blive anmodet om fra en tilsynsmyndighed.

Når først en repræsentant er blevet identificeret, skal du skriftligt udpege denne person som din organisations repræsentant. En repræsentant repræsenterer DPO'eren eller databehandleren med hensyn til deres respektive forpligtelser i henhold til GDPR.

Et par noter om repræsentanter:

- En repræsentant skal være etableret i en af de EU-medlemsstater, hvor dine datasubjekter er placeret
- Det er dit ansvar at udnævne en repræsentant, som ikke har fordomme overfor eventuelle juridiske handlinger, der kunne blive indledt mod din virksomhed.
- En repræsentant vil blive underlagt enhver tvangsfuldbyrdelse i tilfælde af manglende efterlevelse fra virksomhedens side. Det betyder, at både din virksomhed og din repræsentant kan blive straffet, hvis du ikke overholder loven.



Som GDPR nærmer sig, dukker der masser af serviceydelser op i EU for organisationer, der skal udpege repræsentanter.

Næste trin

For at forberede til GDPR, er det vigtigt at forstå, hvilke data du opretter, hvor og hvordan du behandler og gemmer dem, og hvordan din organisation kan understøtte brugernes rettigheder i dine systemer.

Vi anbefaler, at du begynder med at identificere, hvordan personoplysningerne strømmer igennem dit website.

Når først du har identificeret, hvilke data du bruger og hvordan, kan du begynde at oprette systemer for bedre at beskytte brugerens privatliv og opbygge processer, så brugere kan få adgang til at opdatere eller fjerne deres data fra dine systemer.

Har du brug for hjælp til nogle af trinene i at overholde de nye regler, så kontakt FFW. Vi tilbyder en GDPR Compliance pakke, der analyserer din digitale tilstedeværelse for at finde potentielle overensstemmelsesproblemer, og vi giver anbefalinger til oprydning af data.

Kontakt os for at komme i gang med at reducere risikoen for store bøder i henhold til loven. En af vores GDPR eksperter vil kontakte dig for at hjælpe dig med at finde ud af, hvordan du kan bevæge dig fremad.