WHITEPAPER

GDPR-COMPLIANT MET EEN CONCRETE AANPAK:

TIJDLIJN EN STAPPEN VOOR BEDRIJVEN VAN IEDERE OMVANG.

Auteurs:
Wessel Veltman
Jelmer Pieters

ENJOY SAFER TECHNOLOGY™

DPO Consultancy
Experts in Data Protection

INHOUD

Introductie . . . 2

1. Wat is de GDPR en wat betekent het voor organisaties? . . . 3

1.2 Waarborgen van bescherming van persoonsgegevens . . . 3

1.2 GDPR in de praktijk . . . 3

2. Waar moet een organisatie rekening mee houden om te voldoen aan de nieuwe wetgeving? 4

2.1 Scope van de maatregelen . . . 4

2.2 Wie in de organisatie zijn betrokken bij de GDPR? . . . 4

2.3 Minimale technische vereisten . . . 5

2.4 Wat wordt er naast basisbeveiliging verwacht van organisaties? . . . 7

3. Concreet stappenplan . . . 8

Stap 1 - Nulmeting met gap-analyse . . . 8

Stap 2 - Implementatieplan . . . 8

Stap 3 - Implementatie . . . 8

Stap 4 - Beheer . . . 8

4. Conclusie . . . 9

5. Over ESET & DPO Consultancy . . . 10

INTRODUCTIE

De **General Data Protection Regulation (GDPR)**, ook bekend als de **Algemene Verordening Gegevensbescherming (AVG)**, is in de hele Europese Unie de nieuwe standaard voor het beschermen van persoonsgegevens.De wet geldt voor alle organisaties en personen die in de Europese Unie (EU) zijn gevestigd en persoonsgegevens verwerken en voor alle organisaties en personen die buiten de EU zijn gevestigd en gegevens verwerken van burgers in de EU.

Wanneer de GDPR van toepassing is op een organisatie zal zij met de GDPR compliant moeten zijn, en als dat nog niet het geval is, aan de slag moeten om compliant te worden en te blijven. Deze whitepaper, geschreven in samenwerking met DPO Consultancy, is er om de GDPR toe te lichten en om te informeren over wat vereist is om compliant te zijn: wat moet een organisatie ondernemen om aan de wetgeving te voldoen? Wie in de organisatie zijn erbij betrokken? Waar moet een organisatie rekening mee houden en wat zijn minimale vereisten? Op basis van deze informatie presenteren we een concreet stappenplan die helpt bij de implementatie van de GDPR binnen de dagelijkse praktijk van het bedrijf.

1. WAT IS DE GDPR EN WAT BETEKENT HET VOOR ORGANISATIES?

1.1 WAARBORGEN VAN BESCHERMING VAN PERSOONSGEGEVENS

De GDPR regelt de bescherming van persoonsgegevens. De bescherming van persoonsgegevens is een grondrecht dat is vastgelegd in het Handvest van de Grondrechten van de Europese Unie en in het Verdrag betreffende de werking van de Europese Unie. De GDPR wil twee belangen waarborgen. Ten eerste, de bescherming van natuurlijke personen in verband met de verwerking van hun gegevens, en ten tweede het mogelijk maken van het vrije verkeer van persoonsgegevens binnen de Europese Unie (EU). Het waarborgen van deze twee belangen vraagt voortdurend een afweging van de belangen van degene wiens gegevens worden verwerkt en van de belangen van de organisatie die de gegevens verwerkt. Met de opkomst van de digitalisering zijn de belangen van degenen wiens gegevens worden verwerkt steeds meer onder druk komen te staan en lijkt het erop dat men dat vergeten is, waardoor de grondrechten van burgers in het geding komen. Niet alleen het grondrecht op privacy, maar praktisch alle grondrechten.

De GDPR is vanaf **25 mei 2018** rechtstreeks toepasselijk binnen de gehele EU en vervangt de Nederlandse Wet bescherming persoonsgegevens (Wbp). Voor wat betreft de belangen die de GDPR wil waarborgen is er geen verschil met de Wbp. En op het gebied van gegevensverwerking zijn er heel weinig nieuwigheden in de GDPR. Maar in één opzicht is de GDPR fundamenteel anders dan de Wbp. En dat betreft alles wat een gegevensverwerkende organisatie moet doen om ervoor te zorgen dat zij het beschermen van persoonsgegevens structureel waarborgt ('compliance') én daarover ook verantwoording kan afleggen en aflegt ('accountability'). Dit vraagt van vrijwel alle organisaties veel tijd, geld en energie, en vaak ook een cultuuromslag. In samenwerking met Mazars hebben wij eind 2016 een whitepaper gepubliceerd dat ingaat op de regels van de wet. Deze vind je hier.

Vooral met deze verantwoordingsplicht leveren organisaties een belangrijke bijdrage aan de bescherming van het grondrecht op privacy. De gevolgen voor een organisatie wanneer zij niet voldoet aan eisen van de wet kunnen fors zijn. Denk hierbij aan flinke boetes, maar vooral ook aan imagoschade, klantverlies en minder business. Een ander bijzonder verschijnsel dat we waarnemen in de aanloop naar de intrede van de GDPR, is dat klanten en leveranciers elkaar kritisch bevragen over hoe zij omgaan met persoonsgegevens. U doet het dus niet alleen om boetes te voorkomen, maar vooral om te laten zien dat u het vertrouwen van uw relaties op waarde schat door daadwerkelijk zorgvuldig met hun belangen om te gaan.

Samengevat: voldoen aan de GDPR vraagt een forse inspanning en kost geld, maar per saldo levert het veel meer op dan dat het kost: imagobehoud/-versterking, meer en meer tevreden klanten en business partners, daardoor meer business en betere rendementen, en dus extra waarborgen voor de continuïteit van uw bedrijf.

1.2 GDPR IN DE PRAKTIJK

Bedrijven en andere organisaties die nog niet aan de GDPR voldoen zullen aan de bak moeten, want per 25 mei is de GDPR onverkort van toepassing en is de Autoriteit Persoonsgegevens, de nationale toezichthouder, gehouden de wet te handhaven. In de praktijk blijkt echter dat dit voor veel organisaties niet gemakkelijk is.

Eén van de achtergronden hiervan is, dat de GDPR een wet is die diep ingrijpt in organisaties, complex geformuleerd is, en veel open begrippen en vage normen bevat. Bedrijven zullen zelf aan de slag moeten gaan met het concreet invulling geven aan de eisen die de wet aan hen stelt. Die invulling kan van bedrijf tot bedrijf verschillen. De wet eist dat een bedrijf 'passende technische en organisatorische maatregelen' treft. Passende maatregelen zijn afhankelijk van de context waarin persoonlijke data wordt verwerkt en opgeslagen. Mede door ontoereikende kennis is het voor bedrijven lastig om de vertaalslag te maken naar de praktische implementatie van wat de wet eist.

2. WAAR MOET EEN ORGANISATIE REKENING MEE HOUDEN OM TE VOLDOEN AAN DE NIEUWE WETGEVING?

2.1 SCOPE VAN DE MAATREGELEN

'Passende technische en organisatorische maatregelen' omvat meer dan maatregelen op het gebied van IT (waaronder IT-security), respectievelijk allerlei meer juridisch en procedureel getinte maatregelen. Alles valt of staat met een organisatie die op een bewuste en verantwoorde manier met persoonsgegevens omgaat. Bij het treffen van maatregelen is aandacht voor het aspect van bewustwording van de gehele personele organisatie van belang. In dat kader speelt onder meer het vraagstuk van de ethiek. Het gaat dan niet om de – juridische – vraag of een bepaalde verwerking wel of niet is toegestaan, maar om meer morele vragen zoals: moeten we bepaalde verwerkingen eigenlijk wel willen? Waar leggen we onszelf beperkingen op vanuit een meer maatschappelijk gedreven gedachte of overtuiging?

Het perspectief van waaruit naar de bescherming van persoonsgegevens gekeken dient te worden, behoort sowieso juridisch/organisatorisch ofwel IT-technisch te zijn. De GDPR nodigt uit om vanuit een ander, veel breder perspectief met de materie aan de slag te gaan, namelijk het informatieve perspectief. Oftewel: uitgaan van het principe van 'follow the data'. De GDPR definieert immers persoonsgegevens niet anders dan als een bepaalde vorm van informatie. Vanuit dat brede informatieve perspectief met de bescherming van persoonsgegevens aan de slag gaan, omvat dan ook meer dan de doorgaans gebruikelijke interpretatie van 'technische en organisatorische maatregelen', en levert een substantieel meer solide resultaat op.

2.2 WIE IN DE ORGANISATIE ZIJN BETROKKEN BIJ DE GDPR?

In een bedrijf kan niet één iemand verantwoordelijk zijn voor de GDPR. De hele organisatie heeft er immers mee te maken en iedereen draagt medeverantwoordelijkheid. De volgende organisatieonderdelen zijn in elk geval betrokken bij de (implementatie van de) GDPR:

HUMAN RESOURCES (HR)

HR-afdelingen hebben op twee manieren te maken met de GDPR. Ten eerste als verwerker van informatie van medewerkers. Er dient in kaart te worden gebracht welke gegevens worden verwerkt hoe deze worden verwerkt. En uiteraard dienen er in dat kader de nodige maatregelen getroffen te worden (zoals een register van verwerkingen). Ten tweede om vorm en inhoud te geven aan dat deel van het personeelsbeleid dat toeziet op de bewustwording van de personele organisatie (denk aan: trainingen en coaching).

LEGAL

Bedrijfsjuristen hebben vanzelfsprekend te maken met de GDPR aangezien het wetgeving betreft en zullen moeten adviseren over de wet en de juridische implicaties ervan voor de bedrijfsvoering. Daarnaast hebben zij een monitorende verantwoordelijkheid voor wat betreft nieuw te verschijnen wetgeving, en ook bij het geven van trainingen/workshops aan personeel voor wat betreft de meer technisch-juridische aspecten van de wetgeving.

SALES EN MARKETING

Accountmanagers en marketeers zullen vooral rekening moeten houden met de eisen die de wet stelt aan het opvragen, bewerken en bewaren van persoonsgegevens. Organisaties mogen persoonsgegevens uitsluitend gebruiken voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen, en dan alleen nog maar voor zover het gebruik noodzakelijk is voor het doel van de operatie.

ICT

De ICT-afdeling en de externe partner(s) van het bedrijf zijn betrokken bij de ICT-technische implementatie die de GDPR vereist én het onderhouden van de ICT systemen en in het bijzonder de beveiliging ervan. De ICT-afdeling zorgt onder meer voor het formuleren van IT-beleid op het gebied van data protectie en het hiervan af te leiden IT-security beleid, het managen van de data infrastructuur en het voldoen aan de operationele ICT-vereisten, denk hierbij aan het monitoren, reviewen en testen van data verwerkingsprocedures en het inrichten, testen, operationaliseren, monitoren en onderhouden van de ICT-beveiliging. Maar ook zal zij een belangrijke bijdrage moeten leveren aan een actieplan wanneer er een beveiligingsincident zoals een datalek plaatsvindt.

BESTUUR/DIRECTIE

Het bestuur c.q. de directie is verantwoordelijk voor het – verplicht op te stellen – privacybeleid en voor de privacy governance (kort gezegd: het stelsel van sturen, beheersen, toezicht houden en verantwoorden van alles wat met de GDPR te maken heeft). Het bestuur/de directie faciliteert de organisatorische inbedding van alle te nemen maatregelen, en de eindverantwoordelijke bestuurder/directeur is rechtstreeks aanspreekbaar voor de eventueel aangestelde functionaris gegevensbescherming en/of voor de AP voor wat betreft het door de organisatie voldoen aan de eisen die de GDPR stelt.

2.3 MINIMALE TECHNISCHE VEREISTEN

Een belangrijk onderdeel van de GDPR is de beveiliging van data. Wat ons betreft bestaat de basisbeveiliging in de meeste gevallen ten minste uit de volgende maatregelen:

ANTI-MALWARE

ook wel endpoint security genoemd

Dit gaat verder dan enkel antivirus. Een goede Endpoint Security oplossing past meerlaagse technologie toe die malware uitbraken, misbruik van (bekende) kwetsbaarheden, netwerkaanvallen, versleuteling door ransomware en meer helpt voorkomen.

FIREWALL

(zowel op netwerk- als op endpointniveau)

Netwerkfirewalls blijven de hoeksteen van netwerkbeveiliging en zijn misschien wel de belangrijkste investering die een bedrijf kan doen. Basis firewalls bieden port-filtering en blokkeren schadelijk netwerkverkeer. De geavanceerdere firewalls, ook wel als 'next generation' bestempeld, bieden geavanceerde inspectie van het netwerkverkeer, inclusief anti-malware bescherming, content filtering, inbraakdetectie en -preventie en threat intelligence. Netwerkfirewalls bieden een goede basisbeveiliging binnen de bedrijfsomgeving. Veel bedrijven schenken echter nog te weinig aandacht op de firewall van de endpoints die zich buiten het netwerk bevinden, zoals thuiswerkers of medewerkers die buiten de deur werken. Met een intelligente firewall op de laptops met in- en uitbraakdetectie en preventie binnen een endpoint security oplossing, zijn alle apparaten ook buiten het netwerk goed beveiligd tegen bedreigingen vanaf het internet en buitenaf.

BACKUP & RECOVERY

Het klinkt misschien logisch, maar als data corrupt raakt op een systeem, dan is het hebben van een recente back-up waarschijnlijk je grootste redding. Het is belangrijk dat u kunt uitsluiten dat de back-up niet corrupt is. Laat u hiervoor adviseren door een IT-specialist.

RECHTENBEHEER

Moet elke medewerker overal bij kunnen? Het is essentieel dat u hier grondige keuzes in maakt om de kans op menselijke fouten te verkleinen.

WACHTWOORDBELEID

Er zijn inmiddels legio manieren waarop u kunt inloggen op systemen. Echter blijft het gebruiken van een wachtwoord, al is het optie B naast het inloggen met je vingerafdruk, in de meeste gevallen nodig. Lengte van een wachtwoord is belangrijker dan complexiteit. Word dus handig in het verzinnen van wachtwoordzinnen, en overweeg een goede wachtwoordkluis zodat al die wachtwoorden hoeft te onthouden.

UPDATES

(operating system, software, browser en browser plug-ins)

Van uitstel komt afstel? Hoe vervelend het moment soms is waarop de update-melding komt, zorg ervoor dat alle collega's het belang inzien van regelmatig updaten en overweeg een patchmanagementoplossing te implementeren die veel werk eenvoudiger kan maken.

VEILIGE BROWSERINRICHTING

Kies een browser waar iedereen mee mag werken en voorkom dat collega's eigen browsers mogen installeren. Ook het updaten moet (bij voorkeur automatisch) kunnen worden afgedwongen.

VEILIGE E-MAILINRICHTING EN –GEBRUIK

Veel datalekken ontstaan door het onbedoeld delen van gevoelige informatie met de verkeerde ontvanger. Ook een mail uitsturen naar een grote groep ontvangers waarbij alle adressen in het Aan of CC-veld in plaats van BCC-veld worden geplaatst brengt het risico van een datalek met zich mee. Zorg ervoor dat iedereen zich hiervan bewust is bij het delen van een bestand met gevoelige informatie. Het instellen van een vertraging van bijvoorbeeld 2 of 5 minuten voordat de mail de server verlaat, kan hierin ook een uitkomst zijn. Bij voorkeur deel je helemaal geen bestanden meer via de mail maar plaats je deze op een bestandsdelingspagina met een goed wachtwoord op de downloadlink en een maximale tijd dat de link actief is.

VEILIGE NETWERK- EN WIFI-INRICHTING

Geen enkel bedrijf kan werken zonder een bedrijfsnetwerk. Of dit nu een lokaal netwerk en servers betreft, services vanuit de cloud of een hybride aanpak. Het maakt bedrijfsgegevens, applicaties of diensten toegankelijk voor medewerkers en combineert dit in de meeste gevallen met het beschikbaar stellen van draadloze verbindingen via Wifi. Veel netwerken zijn inmiddels vele jaren geleden opgebouwd zonder goede segmentatie. Hierbovenop zijn Wifi accesspoints geschroefd met in de beste gevallen een draadloos "gasten" netwerk met apart Wifi wachtwoord. Een essentiële stap voor een veilig netwerk is het zorgvuldig segmenteren hiervan zodat er bijvoorbeeld een duidelijke (fysieke) scheiding ontstaat van bedrijfskritische serveromgevingen van de reguliere endpoints in het netwerk. In combinatie met goed Wifi-toegangsbeheer en toestelbeleid kunnen alle draadloze apparaten zorgeloos worden toegelaten op het netwerk of gecontroleerde toegang krijgen tot bedrijfsgegevens.

MEERFACTORAUTHENTICATIE

Een van de meest eenvoudige en budgetvriendelijke oplossingen die veel toevoegen aan uw beveiliging is het toepassen van meer- of tweefactorauthenticatie. Naast uw gebruikersnaam en wachtwoord (iets wat u weet) gebruikt u er een eenmalige code naast die bijvoorbeeld uit een app op uw smartphone wordt gehaald (iets wat u heeft). Er zijn genoeg gebruiksvriendelijke vormen die het inloggen niet ingewikkelder maken voor gebruikers.

ENCRYPTIE

(at rest en in transit)

De GDPR rept hierover in relatie tot bijzondere persoonsgegevens. Beschouw het als uw laatste verdedigingslinie. Als data al op straat ligt, dan kan niemand er wat mee als deze data is versleuteld. Een veelgebruikte toepassing is het versleutelen van harde schijven in laptops. Voeg hier degelijke logging en monitoring aan toe en u voorkomt de vervelende datalek scenario's waarbij data via een laptop of externe media onbedoeld op straat komt te liggen.

EEN DEGELIJK LOGGINGBELEID

Veel software die wordt gebruikt, logt waarschijnlijk al of biedt deze functionaliteit aan maar staat niet ingeschakeld. Inventariseer van alle applicaties waar persoonsgegevens doorheen gaan of en hoe deze applicaties kunnen loggen en help uzelf met periodiek inzicht. Als er dan een incident plaatsvindt dan kunnen de logs u meer vertellen over de oorzaak en oorsprong van het incident. Uiteraard kunnen ook beveiligingsoplossingen hier een belangrijke rol is spelen. Deze bewijslast is een vereiste vanuit de GDPR.

De hiervoor genoemde voorbeelden zijn niet de heilige graal, echter verkleint u de kans op beveiligingsincidenten aanzienlijk door hier stappen in te nemen.

2.4 WAT WORDT ER NAAST BASISBEVEILIGING VERWACHT VAN ORGANISATIES?

Het is belangrijk dat de ICT-systemen op orde zijn, maar wanneer een bedrijf GDPR-proof wil zijn, dient het ook zorg te dragen voor een veelheid aan andere maatregelen. Denk hierbij aan de volgende:

- Gedocumenteerd intern privacybeleid
- Gedocumenteerd Information Security beleid;
- Opleiden en trainen van medewerkers
- Functionaris voor Gegevensbescherming (Data Protection Officer)
- Interne en extern communicatiebeleid
- Privacy statements
- Data Protection Impact Assessment-procedure (DPIA);
- Risico inventarisatie;
- Netwerksegmentatie;
- Logging / monitoring;
- Security & Privacy by design én by default;
- Periodieke audits;
- Penetratie testen (ook periodiek);
- Incident Response Plan;
- Verwerkersovereenkomsten;
- Register(s) van verwerkingen.

In onze optiek spelen de business partners, waaronder de ICT-partners, een belangrijke rol in het (mede) zorgdragen voor het voldoen aan de eisen van de GDPR en dus voor bovenstaande zaken. Omdat ICT naast het op orde brengen van de systemen een belangrijke rol speelt bij diverse van de bovenstaande punten, hebben ICT-partners de juiste kennis van de GDPR nodig om op ICT-gebied aan jouw organisatie de juiste begeleiding te bieden.

3. CONCREET STAPPENPLAN

De grote vraag die speelt bij bedrijven in Nederland is hoe ze de GDPR nu praktisch vorm en inhoud kunnen geven. Om compliant te worden en te blijven is allereerst inzicht nodig in de eigen organisatie. Met de verkregen informatie kan een plan van aanpak worden opgesteld waarmee de nodige maatregelen geïmplementeerd kunnen worden. Onderstaand is op hoofdlijnen een stappenplan weergegeven.

STAP 1 NULMETING MET GAP-ANALYSE

Tijdens de eerste stap wordt grondig getoetst en vastgesteld in welke mate de organisatie aan de eisen van de GDPR voldoet. Er wordt een overzicht opgesteld van mogelijke risico's waar de organisatie mee te maken kan krijgen in het kader van het verwerken van persoonsgegevens. Een gedegen inventarisatie zorgt voor het juiste inzicht en legt ook direct de pijnpunten bloot. Deze pijnpunten vormen het uitgangspunt voor de gap analyse. Het doel van de gap analyse is om de afstand te zien van de huidige stand van de organisatie tot de vereisten vanuit de wet, waaronder op het gebeid van het gewenste beveiligingsniveau.

STAP 2 IMPLEMENTATIEPLAN

Het borgen van privacy gaat door de hele organisatie heen. Dit komt duidelijk naar voren in het implementatieplan; het is erop gericht om op een gestructureerde en beheerste manier de te nemen maatregelen in de bedrijfsvoering in te voeren en te borgen. Een implementatie slaagt alleen als alle afdelingen bij elke stap worden betrokken en constructief deelnemen. Het implementatieplan voorziet niet alleen in het creëren van draagvlak maar ook in het vormen van een projectteam. Een plan zorgt ervoor dat iedereen weet wat er moet gebeuren, wie wat wanneer moet opleveren, met welke kwaliteit, wat de prioriteiten zijn en hoe de implementatie op een zorgvuldige en beheerste manier plaats vindt.

STAP 3 IMPLEMENTATIE

Tijdens deze fase komt het plan tot leven. Elke stakeholder heeft zijn verantwoordelijkheden en doelstellingen. De projectleider houdt milestones en deadlines in de gaten en stuurt bij wanneer nodig. Het is zeer aan te raden om tweewekelijks of maandelijks naar de gehele organisatie te rapporteren op voortgang van het project. Het belang van privacybewust werken moet geborgd blijven binnen alle afdelingen.

STAP 4 BEHEER

En dan is het project afgerond en zul je na de implementatie GDPR proof willen blijven. Dat is een doorlopend proces, aangezien de wet kan veranderen, er nieuwe wetten kunnen verschijnen, de organisatie kan veranderen en zo meer. Het adequaat belegd hebben van privacy governance is dan ook essentieel. Dat betreft niet alleen de management aspecten van het privacybeleid, maar onder meer ook het interne toezicht, waaronder via een – eventueel verplicht – aan te stellen Functionaris voor Gegevensbescherming (FG/DPO).

4. CONCLUSIE

Op 25 mei zal de GDPR rechtstreeks van toepassing zijn in de gehele EU. Organisaties die aan de slag willen met de GDPR zullen meer moeten doen dan alleen het afvinken van lijstjes met procedurele en technische maatregelen. Om compliant te zijn dient een bedrijf niet alleen zijn systemen op orde te hebben; ook organisatorisch moeten er de nodige maatregelen worden getroffen, waaronder op het gebied van bewustwording, in welk kader ook ethische kwesties aan bod komen. In de organisatie van een bedrijf is bijna iedereen betrokken bij het (blijven) voldoen aan de eisen die de GDPR stelt.

ESET heeft in samenwerking met DPO Consultancy dit stappenplan naar GDPR-compliance opgesteld. Het volgen van het stappenplan biedt organisaties een goede praktische leidraad om zicht te krijgen op en inzicht in te krijgen in de huidige stand van zaken en om op basis van een gestructureerde, efficiënte en effectieve aanpak zo spoedig mogelijk GDPR-compliant te worden. ESET, DPO Consultancy en hun business partners zijn uw bedrijf graag van dienst om aan de invulling van dit stappenplan vorm en inhoud te geven.

GDPR compliant worden is voor veel organisaties een uitdaging, daarom helpen we u graag op weg. Meld u aan voor de GDPR podcast waar we aan de hand van concrete voorbeelden de IT-uitdagingen bespreken en u proberen handvatten te geven waarmee u direct aan de slag kunt.

MELD U AAN VOOR DE GDPR PODCAST

5. OVER ESET & DPO CONSULTANCY

ENJOY SAFER TECHNOLOGY™

Al 30 jaar lang ontwikkelt ESET® toonaangevende IT-beveiligingssoftware en -diensten voor bedrijven en consumenten over de hele wereld. Inmiddels is ESET uitgegroeid tot het grootste IT-security bedrijf van de Europese Unie met oplossingen variërend van endpoint en mobile security, tot encryptie en tweefactorauthenticatie. ESET beschermt en monitort 24/7 op de achtergrond en werkt beveiliging in real-time bij om gebruikers veilig te houden en bedrijven zonder onderbreking te laten werken.

Als expert in dataprotectie adviseren wij onze partners, bedrijven en consumenten over de GDPR en de implicaties hiervan. Dit doen wij door het aanbieden van content, educatie en technologie.

DPO Consultancy
Experts in Data Protection

Voor veel organisaties vormt het GDPR-compliant worden en blijven een enorme uitdaging. Het ontbreekt doorgaans aan de vereiste expertise (kennis, kunde en vaardigheid) en aan de noodzakelijke capaciteit om de eigen organisatie compliant te maken én te houden.

Anders dan andersoortige aanbieders van diensten op dit gebied, zoals advocatenkantoren, ICT-leveranciers en accountantskantoren, legt DPO Consultancy zich uitsluitend toe op het begeleiden van organisaties bij het realiseren van hun dataprivacy uitdagingen, waaronder GDPR-compliant worden en blijven. Ons vak is privacy management.

Ons team bestaat uit zeer ervaren professionals op het gebied van privacy management in het algemeen en gegevensbescherming in het bijzonder. Daarnaast onderscheiden wij ons door een integrale, pragmatische maatwerk-aanpak van alle aspecten van het privacy management: de techniek, administratieve en procedurele aspecten, bewustwording en cultuur, en profilering en communicatie.