Xcellent

WHITEPAPER

OP WEG IN GDPR-LAND

Zo voldoet jouw organisatie aan de nieuwe privacywet

Het vertrekpunt: betrokkenheid van bovenaf

Niemand gaat op reis zonder doel. Vraag je voor vertrek af: waar willen we naartoe? Hoe belangrijk is gegevensbescherming voor ons bedrijf? Doen we het alleen voor het vinkje, zodat we aan de wet voldoen en problemen voorkomen? Vanuit intrinsieke motivatie, om de privacy van onze klanten goed te beschermen? Of trekken we GDPR breder en gebruiken we het als hefboom om bijvoorbeeld interne processen te verbeteren? Met andere woorden: zien we het als noodzakelijk kwaad of als een kans om ons te onderscheiden van concurrenten?

Het zijn vragen die strategische beslissers binnen bedrijven moeten beantwoorden. Het begint bij hun betrokkenheid. Commitment. Lange tijd is er veel ontwijkend gedrag vertoond. GDPR? Komt wel. Of: het zal zo'n vaart niet lopen. Een andere veelgehoorde reactie: dat geldt niet voor ons, toch?

Die tijd is voorbij nu de GDPR sinds 25 mei 2018 daadwerkelijk van kracht is geworden. Je kunt ervoor kiezen om geen maatregelen te nemen, maar dan moet je het ook kunnen uitleggen als het fout gaat. De Autoriteit Persoonsgegevens (AP) kan een datalek dan beoordelen als nalatigheid en bestuurders persoonlijk aansprakelijk stellen. Waarom zou je het zover laten komen?

Formeer een projectgroep

Betrokkenheid is één, aan de slag gaan twee. Hoe begin je aan de reis naar een organisatie die GDPR-proof is? Start met het formeren van een projectgroep. Waarom is dat belangrijk en wie moeten daar dan in?

Mens, techniek en proces. Die drie essentiële pijlers binnen bedrijven hebben allemaal veel met data te maken. En moeten dus vertegenwoordigd zijn binnen de projectgroep. Zo is een HR-specialist, die zich zowel met mensen als met processen bezighoudt, onmisbaar. IT heeft verstand van techniek en is logischerwijs ook aan boord. Een afvaardiging van de directie is uiteraard ook aanwezig en brengt strategisch inzicht mee. Maar denk ook aan een marketeer, die vaak met data werkt, en andere disciplines binnen je bedrijf. Betrek in elk geval een juridisch expert bij je projectgroep. Bij voorkeur iemand die gespecialiseerd is in IT-recht en privacy.

Functionaris gegevensbescherming: de reisleider

Wie gaat de interne GDPR-reis leiden? Een Functionaris voor de gegevensbescherming is dé gegadigde. Niet voor elke organisatie verplicht, maar voor de meeste wel aan te bevelen. Het advies luidt: 0,1 fte per 100 medewerkers in een 'onderhoudssituatie', als het traject al even loopt. In de intensievere projectfase moet de functionaris meer meters maken. Een organisatie met 1000 medewerkers kan dus prima een fulltime functionaris voor de gegevensbescherming aanstellen.

Voor bedrijven die geen fulltime functionaris in dienst hebben ligt het voor de hand er een in te huren. Het is alleen maar sterk dat je laat zien dat iemand met de juiste kennis en vaardigheden aan het roer staat van jouw GDPR-projectgroep. Maak je helemaal niemand verantwoordelijk voor het welslagen van jullie expeditie, dan is de kans groot dat het eindpunt nooit bereikt wordt.

Verwerkingsregister: de GDPR-landkaart

Het doel is bepaald, het team geformeerd. Het GDPR-landschap strekt zich voor je uit en het startschot klinkt. Rijst de vraag: welke route leg je af? En waar te beginnen?

Het antwoord luidt: met het opstellen van een verwerkingsregister. Dat is de plattegrond waarop je alle dataverwerkingen binnen je organisatie in kaart brengt. De meest belangrijke stap in het hele proces. Met deze GDPR-landkaart toon je precies aan wie waar welke persoonsgegevens verwerkt. Dit document is de basis van al je verdere stappen en acties en bovendien voor de meeste organisaties verplicht. De GDPR-landkaart geeft weer welke data je verzamelt, voor welk doel, hoe gevoelig die gegevens zijn, hoe je ermee omgaat en hoe je ermee zou moeten omgaan. Ook toont deze 'plattegrond' aan om welke categorieën van betrokkenen (klanten, patiënten, etc.) en persoonsgegevens (NAW, IP-adres, geboortedatum, etc.) het gaat, wat de bewaartermijnen zijn, met wie je de gegevens deelt en hoe je ze beveiligt.

Datalek? Altijd melden!

Een datalek, en dan? In Nederland waren bedrijven al verplicht daarvan melding te maken bij de Autoriteit Persoonsgegevens (AP). Sinds 1 januari 2016 om precies te zijn, toen de meldplicht datalekken in werking trad. De komst van de GDPR verandert daar niets aan, de meldplicht maakt daarvan deel uit.

Binnen 72 uur na ontdekking van het datalek moet het gemeld zijn bij de AP. Dat is kort. Zeker gezien het omvangrijke formulier dat je daarvoor moet invullen. Hoe is het ontstaan? Welke data is er precies gelekt? Hoe lang heeft het lek geduurd? Wie heeft er toegang tot de gegevens gehad? Was het te voorkomen? Is het lek inmiddels gedicht? Wat is het risico voor de betrokkenen? Je hebt snel veel informatie nodig. Dit benadrukt het belang van een verwerkingsregister.

Zwart-op-wit: de verwerkersovereenkomst

Geen enkele organisatie is een eiland. Je werkt samen met leveranciers en klanten. En de kans is groot dat je daarbij data uitwisselt. Dat een leverancier gegevens afkomstig van jouw organisatie verwerkt. Daarom moet je, zeker als het om persoonsgegevens gaat, met al die verwerkers een overeenkomst afsluiten waarin je dat gezamenlijk vastlegt: de verwerkersovereenkomst. Als verantwoordelijke voor de data moet jij immers verantwoording afleggen als de gegevens op straat komen te liggen. Met een verwerkersovereenkomst heb je zwart-op-wit wat de onderlinge afspraken zijn en wat er in zo'n situatie verwacht wordt.

Rechten van betrokkenen

In GDPR-land houd je rekening met de rechten van betrokkenen, zodat zij meer controle hebben over hun persoonsgegevens. Dat is de essentie van de nieuwe privacywet. Betrokkenen hebben recht op inzage van hun data, op correctie ervan en mogen jou als verwerker vragen de data te verwijderen. Ook hebben ze recht op dataportabiliteit; het recht om persoonsgegevens over te dragen, bijvoorbeeld als ze wisselen van tandarts.

Zeker business-to-consumer (B2C) bedrijven kunnen zulke vragen verwachten. Ook dit wijst weer op het grote belang van een goed verwerkingsregister. Dat maakt het gemakkelijk om snel en goed te antwoorden. Op een vraag als 'welke data heb je van mij verzameld?' moet binnen vier weken een inhoudelijk antwoord volgen, tenzij het geen redelijk of realistisch verzoek is. Maar meestal moet je het vrij snel kunnen oplepelen.

De rode draad door je GDPR-reis: verantwoorden!

Stel dat je data moet verwijderen, dan moet je vervolgens ook kunnen aantonen dat je dat daadwerkelijk gedaan hebt. Dit heeft alles te maken met de verantwoordingsplicht die je als verwerker van persoonsgegevens hebt. Het is de rode draad door je GDPR-reis: verantwoorden! Waarom sla je data wel of niet op? Als je het doet, dan moet dat op basis van een van de wettelijke grondslagen gebeuren. Laat zien dat je toestemming hebt. Neem dit serieus, sla het niet in de wind. Wie zegt data te verwijderen maar het vervolgens niet doet, valt voor de AP in de zwaarste categorie van boetes.

Onderdeel van de verantwoordingsplicht is ook een lijst van preventiemaatregelen, zowel technische (van firewalls tot rechtenmanagement) als organisatorische. Laat zien dat je de risico's onderkent en de juiste maatregelen genomen hebt. Doet er zich toch een beveiligingsincident voor, dan ben je verplicht dat te registreren. Óók de incidenten die niet direct met persoonsgegevens te maken hebben. Wees eerlijk en geef openheid van zaken om erger te voorkomen.

Volgende halte: het privacystatement

Je bent goed op weg. Volgende halte: het privacystatement. De GDPR brengt een informatieplicht met zich mee die zegt dat je betrokkenen moet informeren over de data die je over hen verzamelt. Waarom verzamel je die? En met wie deel je de gegevens? Antwoorden op zulke vragen moeten terugkomen in het privacystatement op je website. Zijn er alsnog onduidelijkheden dan zou de Functionaris Gegevensbescherming beanderbaar moeten zijn als contactpersoon.

Vaak zijn zulke documenten lang en wollig. In dit geval moet de tekst juist bondig, to-the-point en duidelijk zijn. Voor iedereen te begrijpen. Tip: zet er een copywriter op. Transparantie in je communicatie is een verplichting vanuit de nieuwe privacywet.

Cookies, verhaal apart binnen de GDPR

Op dit moment nog een verhaal apart binnen de GDPR zijn cookies, de kleine bestandjes die vanuit een website op je computer worden geplaatst om je internetgedrag te volgen. Ze vallen namelijk nog niet voor honderd procent onder de nieuwe privacywet. Nu krijgt iedereen die een website bezoekt nog regelmatig de melding 'Cookies toestaan?' Straks is elke organisatie verplicht in het 'toestaan-scherm' onderscheid aan te brengen in functionele, analytische en social media-cookies. Dat geeft gebruikers van websites meer controle over hun data.

TIP:
nu je toch bezig bent met technische en organisatorische maatregelen voor de GDPR, pak het nieuwe cookiegebruik alvast mee. Hoe? Je kunt zelf bijvoorbeeld gebruikmaken van de handige tool CookieInfo (www.cookieinfo.net). Of je neemt een communicatie- of marketingbureau in de arm. Die weten over het algemeen van de hoed en de rand.

Leeg je bagagetas, verwijder onnodige data!

Het is goed om de bagagetas onderweg te ontdoen van onnodige ballast. Sterker nog: de GDPR eist dat van organisaties. Dat wordt dataminimalisatie genoemd: verzamel niet meer gegevens dan nodig en heb je gegevens waarover je volgens de GDPR niet mag beschikken, verwijder ze dan.

Door de jaren heen hebben bedrijven onmetelijk veel data verzameld. Soms terecht, vaak ook niet. Als jij een nieuwsbrief wil versturen, heb je geen geboortedatum van de ontvanger nodig. Ook geen telefoonnummer of huisadres. Verzamel dat dan ook niet.

Privacy by design & by default

Privacy by design houdt in dat je al bij de ontwikkeling van systemen privacyverhogende maatregelen neemt. Verplaats je in de klant of gebruiker, leef je in. Welke persoonsgegevens heb je werkelijk van diegene nodig en is dat volgens de GDPR rechtmatig?

Waar privacy by design vooral gaat over beveiligingsacties in systemen afdwingen, heeft privacy by default vooral te maken met processen en standaardinstellingen. Voorbeeld: waar voorheen de optie voor het ontvangen van een nieuwsbrief al automatisch was aangevinkt, bijvoorbeeld na een online aankoop door een klant, vereist de GDPR dat je het nu precies andersom inricht. De klant bepaalt zélf of hij de nieuwsbrief wil ontvangen.

Beveiliging: wie kan er bij welke gegevens?

Alleen een wachtwoord is anno 2018 echt te makkelijk. Makkelijk te kraken vooral.
TIP: pas multifactor-authenticatie toe.

Deze vorm van authenticatie kent meerdere lagen en is gebaseerd op iets wat je weet én iets wat je hebt. Mooi voorbeeld is internetbankieren bij Rabobank. Je weet je pincode en je hebt je pinpas. Door je pinpas in de Rabo Scanner te stoppen en de instructies te volgen, krijg je een nieuwe code waarmee je inlogt. Ziedaar de dubbele laag.

Gek genoeg vinden veel organisatie het beveiligingen van mobile devices zoals smartphones en tablets veel minder nodig. Terwijl ze vaak dezelfde toegang tot het bedrijfsnetwerk, applicaties, email en CRM-systemen hebben en daarmee tot allerlei bedrijfs- en persoonsgegevens. Daarbij komt dat het risico op een datalek groter is dan bij vaste werkplekken. Je komt immers buiten de deur met je smartphone en tablet. Ze kunnen makkelijker kwijtraken, gehackt worden of verbinding maken met een gevaarlijk netwerk.

Bestemming bijna bereikt... Maar niet zonder bewustwording!

De GDPR-reis voerde je inmiddels langs organisatorische en technische maatregelen. Je bestemming is na al deze haltes bijna bereikt: een organisatie die GDPR-proof is! Maar... je bent er nog niet.

Alles staat of valt uiteindelijk met bewustwording onder de medewerkers - én daaruit voortvloeiende gedragsveranderingen. Vreemd genoeg worden zeven van de tien datalekken veroorzaakt door menselijke fouten. Meestal door onoplettendheid of onwetendheid. Neem het delen van privacygevoelige documenten. Dat gebeurt nog te vaak per mail en zonder wachtwoord of andere beveiligingsmaatregelen.

Verzeker je tegen mogelijke gevolgschade

Gehoord in de wandelgangen: wij hebben onze organisatie verzekerd tegen de GDPR. Om maar meteen een misverstand weg te nemen: je kunt je niet verzekeren tegen de boete die de AP je eventueel oplegt na het veroorzaken van een datalek. Wél tegen de gevolgschade.

Het is vanuit dat oogpunt zeker aan te bevelen een cyberverzekering te nemen. Door de grootste risico's in kaart te brengen en te elimineren met maatregelen, heb je al veel afgedekt. Maar de kans op restrisico's blijft altijd bestaan.

X

COLOFON

Redactie: Carmen Graauwmans en Martin van der Eijk
Teksten: Thijs Tomassen
Ontwerp en realisatie: doorendoor ontwerp

Xcellent

Voor meer informatie **www.xcellent.nl**

Onderdeel van de Vincere Groep