



WHITEPAPER

GDPR: PLUK ER DE VRUCHTEN VAN

exact.com/nl/gdpr

INHOUD

Introductie	3
Inzicht en efficiency	4
Bedrijfscontinuïteit	5
betere reputatie	6
Onderscheid je positief	7
Je voorkomt hoge boetes	8
Hoe kun je je voorbereiden	9
Hoe kan Exact helpen?	12
Samenvatting	13



INTRODUCTIE

Op 25 mei 2018 treedt de nieuwe Europese privacywet in werking. Het implementeren van deze nieuwe regelgeving zal voor bedrijven extra werk met zich meebrengen, maar ook kansen bieden. Bedrijven die er op tijd klaar voor zijn, weten zeker dat hun continuïteit gewaarborgd is. Ze laten zien dat ze privacy serieus nemen en zullen niet geconfronteerd worden met datalekken en hoge boetes. Maar hoe kun je door de 'risicobomen' heen het 'kansenbos' zien?

Tot 25 mei 2018 heeft elk land in de Europese Unie zijn eigen privacywet. In Nederland is dit de Wet bescherming persoonsgegevens (Wbp). Deze wet, is net als in alle andere Europese lidstaten, tot stand gekomen op basis van de Europese privacyrichtlijn uit 1995. In die tijd was nog maar een kleine groep mensen verbonden met internet, laat staan dat iedereen een smartphone in zijn broekzak had. Daarom heeft de Europese Unie besloten om de privacywetgeving aan te passen, zodat ze beter past in de huidige digitale wereld. Een groot voordeel hiervan is dat er vanaf 25 mei 2018 in de gehele Europese Unie nog maar één

privacywet geldt, in plaats van 28 verschillende nationale wetten.

De volledige naam van de GDPR is de General Data Protection Regulation. In Nederland is deze nieuwe privacywet ook bekend onder de naam Algemene verordening gegevensbescherming (AVG). Dit heeft een impact op de manier waarop we zaken doen. Voor iedereen, van ZZ-P'er tot multinational. Toegegeven, het is heel wat werk, maar realiseer je dat de nieuwe wet ook kansen biedt om je positief te onderscheiden van je concurrenten!

[Bekijk de AVG in een notendop \(pdf\)](#)

KANS 1

INZICHT EN EFFICIENCY

De GDPR vereist dat je een aantal veranderingen doorvoert in de manier waarop je je bedrijfsprocessen en de beveiliging van je informatie organiseert. Dat betekent voor een groot aantal ondernemers dat ze hun bedrijfsprocessen van marketing en sales tot HR moeten bekijken en optimaliseren om zo aan de nieuwe wetgeving te voldoen. Deze GDPR-veranderingen maken je bedrijfsvoering wellicht ook efficiënter. Wanneer je je processen goed op orde hebt, leidt dat tot meer efficiency en een dieper inzicht in je informatie. Je weet nog beter waar je kansen en mogelijkheden liggen.



KANS 2

BEDRIJFSCONTINUÏTEIT DOOR VEILIGHEID

Ongeveer veertig procent van de Nederlandse ondernemers is het afgelopen jaar slachtoffer geweest van cybercrime, aldus schattingen van de politie. Mkb'ers worden vaker getroffen dan multinationals, die meestal meer mensen, kennis en middelen hebben voor digitale beveiliging. Met de opkomst van slimme apparaten, stijgt de gevoeligheid voor cybercrime alleen nog maar verder.

Cybercriminaliteit kan ernstige gevolgen hebben voor bedrijven. Computers, servers en software zijn onmisbaar voor het goed functioneren van je onderneming. Virussen of andere kwaadaardige software (bijvoorbeeld ransomware) kunnen flinke economische schade veroor-

zaken. Voldoe je tijdig aan alle eisen van de GDPR, dan is je bedrijfscontinuïteit beter gewaarborgd en behoeft je jezelf beter voor de problemen die volgen op een datalek of ransomware.



KANS 3

HET ZORGT VOOR EEN BETERE REPUTATIE

Het is de nachtmerrie van elke organisatie om negatief in het nieuws te komen. Klanten zullen het je niet in dank afnemen als hun BSN-nummer en creditcardgegevens op straat belanden. Nieuwe medewerkers zullen niet snel bij je bedrijf solliciteren, wanneer ze net via de media hebben vernomen dat je salarisgegevens van je personeel hebt laten lekken. Door je zaken goed op orde te hebben, blijf je een populair bedrijf voor klanten en een aantrekkelijke werkgever. Kortom, als je de beveiliging van je bedrijf goed op orde hebt en tijdig aan de verplichtingen van de GDPR voldoet, is dat goed voor je bedrijfsimago en -reputatie, waardoor ook de marktwaarde van je onderneming zal toenemen.



KANS 4

ONDERSCHEID JE POSITIEF TEN OPZICHTE VAN JE CONCURRENTEN

Klanten zullen eerder geneigd zijn om te kopen bij een webshop die zijn beveiliging goed op orde heeft en die conform de GDPR met hun gegevens omgaat, dan bij een concurrerende webwinkel waar dat niet het geval is. In deze tijden van fake-news speelt mond-tot-mond-reclame een belangrijke rol. En wat te denken van alle (positieve en negatieve) reviews die mensen op webshops plaatsen? Wanneer jouw klanten en potentiële klanten doorhebben dat jij het goed voor elkaar hebt, en ze twifelen over een concurrent, dan zullen ze eerder bij jou iets aanschaffen. Concurrenten die hun zaken niet goed op orde hebben, geef je dan het nakijken!



KANS 5

JE VOORKOMT HOGE BOETES

Als je voldoet aan de eisen die vanuit de GDPR aan je beveiliging worden gesteld en je overige maatregelen hebt genomen, dan word je niet geconfronteerd met de vaak torenhoge boetes van de Autoriteit Persoonsgegevens (AP). Overtreed je met jouw bedrijf de GDPR, dan kun je een boete krijgen die kan oplopen tot 20 miljoen euro of 4% van je wereldwijde jaaromzet. De kosten om je goed voor te bereiden op de nieuwe wet zijn hier maar een fractie van. Als je je zaken goed op orde hebt, hoef je ook geen “post onvoorzien” aan te houden, omdat je je onzeker voelt. In plaats van dit geld te reserveren, kun je het weer investeren.

BEWERKEN/VERWERKEN

De GDPR is vooral van belang voor organisaties die persoonsgegevens verwerken. Realiseer je dat onder deze nieuwe wet het inzien, bekijken of doorzenden van gegevens al een vorm van verwerken is. Dat geldt niet alleen voor gegevens van je klanten, maar ook voor die van andere relaties en medewerkers. Ook als je het verwerken van gegevens uitbesteedt aan een derde partij, blijf je zelf eindverantwoordelijk voor een correcte omgang met de persoonsgegevens bij deze ketenpartner. Vraag je dus niet af **of** je met de GDPR te maken krijgt, maar **hoe** en **waar in je bedrijf** en **welke maatregelen** je moet nemen.

NB: In de Wet bescherming persoonsgegevens (Wbp) die tot 25 mei 2018 geldt, wordt gesproken over de **bewerker**/verantwoordelijke en een **bewerkersovereenkomst**. In de nieuwe wet die daarna van kracht wordt (de GDPR), heet dit de **verwerker**/**verwerkings**verantwoordelijke en een **verwerkersovereenkomst**. Dit om duidelijk te maken dat ook het opslaan van gegevens, binnen de wet valt.

HOE KUN JE JE VOORBEREIDEN OP DE GDPR?

Alle landen in de Europese Unie hebben een privacy autoriteit die controleert of de huidige en toekomstige privacywetgeving worden nageleefd. In Nederland is dit de Autoriteit Persoonsgegevens (AP). De AP heeft ook een faciliterende rol om organisaties en bedrijven te ondersteunen bij de implementatie van de GDPR. Daartoe heeft de AP onder andere een 10-stappenplan opgesteld aan de hand waarvan je je gedegen kunt voorbereiden op de nieuwe Europese privacywet.

Stap 1

BEWUSTWORDING

Zorg ervoor dat de relevante mensen in je bedrijf, waaronder beleidsmakers en juristen, zich bewust zijn van wat de nieuwe privacyregels inhouden. Zij moeten inschatten

wat de impact van de GDPR is op je huidige processen, diensten en goederen, en welke aanpassingen nodig zijn om aan de nieuwe wet te voldoen. Natuurlijk dient vervolgens iedereen binnen je organisatie op de hoogte te zijn van de nieuwe regels en werkwijze.

Stap 2

RECHTEN VAN BETROKKENEN

Onder de GDPR krijgen mensen van wie je persoonsgegevens verwerkt (klanten, medewerkers en andere relaties) meer en betere privacy-rechten. Zoals onder meer het recht op inzage en het recht op correctie en verwijdering.

Onder de nieuwe wet moet je er ook voor zorgen dat alle mensen van wie je gegevens verzamelt, deze makkelijk van jou kunnen krijgen en deze



kunnen doorgeven aan een andere organisatie wanneer zij dat willen (recht op [dataportabiliteit](#)).

Stap 3

OVERZICHT VERWERKINGEN

Documenteer welke persoonsgegevens je verwerkt en waarom je dit doet, waar ze vandaan komen en met wie je ze gedeeld hebt (verwerkingsregister). Middels [de verantwoordingsplicht](#) schrijft de GDPR voor dat je moet kunnen aantonen dat je bedrijf volgens deze wet handelt. Het verwerkingsregister is bovendien noodzakelijk als klanten, medewerkers of andere relaties hun privacyrechten uitoefenen. Dit is het geval wanneer zij willen dat je hun gegevens aanpast of verwijdert. Dit zal je vervolgens ook moeten doorgeven aan de organisaties waarmee je deze gegevens hebt gedeeld.

Stap 4

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Wanneer het verwerken van persoonsgegevens een hoog privacyrisico kan hebben, dan kun je verplicht zijn om een Data Protection Impact Assessment ([DPIA](#)) uit te voeren. Hiermee kun je vooraf bepalen wat

de risico's zijn en passende maatregelen nemen. Wanneer het niet lukt om dit risico te verkleinen, ben je verplicht om met de Autoriteit Persoonsgegevens te overleggen, voordat je begint met de verwerking. Dit heet de Voorafgaande raadpleging.

Stap 5

PRIVACY BY DESIGN & PRIVACY BY DEFAULT

De GDPR hanteert de uitgangspunten Privacy by Design en Privacy by Default. Zorg ervoor dat je organisatie hier zo snel mogelijk mee vertrouwd raakt. Denk er ook al over na hoe je deze principes kunt invoeren. [Privacy by Design](#) houdt in dat je al bij het ontwerp van producten of diensten rekening houdt met de bescherming van de persoonsgegevens. Zo mag je niet meer gegevens verzamelen, en niet langer, dan voor een specifieke doel nodig is. Privacy by Default betekent dat je technische en organisatorische maatregelen neemt, waardoor standaard alléén die persoonsgegevens verwerkt worden die noodzakelijk zijn voor dat specifieke doel.



Stap 6

FUNCTIONARIS VOOR DE GEGEVENS BESCHERMING (FG)

Het kan zijn dat je onder de GDPR verplicht wordt om een Functionaris voor de gegevensbescherming (FG) aan te stellen. Een FG is een interne privacytoezichthouder voor toepassing en naleving van de GDPR. Overheidsinstanties en publieke organisaties (zoals zorg- en onderwijsinstellingen) dienen altijd een FG aan te stellen. Hetzelfde geldt voor organisaties die vanuit hun kernactiviteiten op grote schaal individuen volgen (bijvoorbeeld via camera-toezicht) of bijzondere persoonsgegevens verwerken, zoals gegevens over iemands gezondheid, ras, politieke opvatting, geloofsovertuiging of strafrechtelijke verleden. Het is raadzaam om zo snel mogelijk te bepalen of jouw organisatie een FG dient aan te stellen. Is dat het geval, werf dan op korte termijn een FG. Is het onduidelijk of jouw organisatie wel of geen FG dient aan te nemen? Neem dan contact op met de AP.

Stap 7

MELDPLICHT DATALEKKEN

De meldplicht datalekken die sinds 1 januari 2016 geldt, blijft onder de

nieuwe GDPR merendeels hetzelfde. Wel worden de registratie-eisen vanaf 28 mei 2018 strenger. Alle datalekken dienen te worden gedocumenteerd, zodat de AP kan controleren of je aan deze meldplicht voldoet.

Stap 8

VERWERKERS- OVEREENKOMSTEN

Heb je je gegevensverwerking uitbesteedt aan een verwerker? Dan dien je te evalueren of de maatregelen die je in het contract met deze verwerker hebt afgesproken (verwerkersovereenkomst) voldoen aan de GDPR. Is dat niet het geval? Dan dien je deze aan te passen aan de nieuwe wet.

Stap 9

LEIDENDE TOEZICHTHOUDER

Heb je ook vestigingen in andere EU-landen dan Nederland? Of heeft je gegevensverwerking invloed in meerdere EU-landen? Dan hoef je nog maar aan één privacytoezichthouder verantwoording af te leggen (de leidende toezichthouder). Zorg wel dat je weet onder welke privacytoezichthouder je bedrijf valt.

Stap 10

TOESTEMMING

Als je toestemming nodig hebt van de mensen van wie je gegevens verwerkt, moet je nagaan of deze toestemming overeenkomstig de GDPR is. Dat geldt zowel voor de manier waarop je toestemming vraagt, als de manier waarop je deze krijgt en registreert. Onder de nieuwe Europese privacywet dien je dit allemaal aan te kunnen tonen. Ook moet het voor mensen net zo eenvoudig zijn om hun toestemming weer in te trekken, als dat ze deze aanvankelijk hebben gegeven.



HOE KAN EXACT HELPEN?

Om als klant van Exact te kunnen voldoen aan de GDPR bieden we in onze software verschillende mogelijkheden om volgens de nieuwe regelgeving met persoonsgegevens om te gaan. Daarnaast ontwikkelen we tools die klanten kunnen helpen te voldoen aan verplichtingen rondom de GDPR.

Deze functionaliteiten kunnen helpen bij het identificeren van persoonsgegevens, zodat je er eventuele acties aan kunt verbinden, zoals verwijderen of anonimiseren. Exact doet dit vanuit zijn rol als softwareleverancier en niet als (juridisch) adviseur. Het voldoen aan geldende wetgeving is, en blijft, de verantwoordelijkheid van jou en je organisatie.

WIL JE MEER INFORMATIE OVER DE GDPR?

- Meld je dan aan voor ons [webinar](#)
- Bezoek de pagina van de [Autoriteit Persoonsgegevens](#) en/of de [EU GDPR](#).



SAMENVATTING

Wanneer iedereen in jouw bedrijf zich realiseert dat de GDPR een belangrijke en zinvolle wet is, zul je er meer draagvlak voor creëren. Medewerkers zullen gemotiveerder zijn om deze privacywet tijdig en correct te implementeren. Ze zullen vervolgens ook eerder bereid zijn om consequent volgens deze nieuwe regels te werken.

Met het stappenplan van de AP kun je al een heel eind komen om je voor te bereiden op de GDPR. Je toont ermee aan dat je zowel de wetgeving als de privacy van je klanten, relaties en medewerkers serieus neemt. Dat levert je veel voordelen op. Het garandeert je bedrijfscontinuïteit, het zorgt voor een betere reputatie, het onderscheid je positief ten opzichte van je concurrenten die het niet zo nauw nemen met de GDPR, je krijgt geen hoge boetes van de AP en je gegevens zijn veilig opgeborgen.

Exact inspireert het mkb om te groeien. Zij dragen de economie, wij ondersteunen ze daarbij. Net als het mkb is Exact niet bang voor het onbekende. We zijn ambitieus en lopen graag voorop. We kennen de uitdagingen en maken software om die te overwinnen. Onze innovatieve oplossingen zijn toegespitst op de bedrijfsbehoeften van onze klanten. Exact biedt het mkb en hun accountants overzicht over vandaag en inzicht in morgen. Zo helpen we onze klanten van over de hele wereld om hun ambities te realiseren.

Exact. Cloud business software.

exact.com/nl/software

Exact Software Nederland B.V.

Molengraaffsingel 33
2629 JD Delft
The Netherlands

T: 0800 - 66 54 631
E: info@exact.nl
www.exact.com/nl

© Exact Group B.V., 2018. Alle rechten voorbehouden. Alle hierin vermelde merk- en handelsnamen behoren toe aan de respectievelijke eigenaren.

= exact