WHITEPAPER

5 ARGUMENTEN WAAROM DE CFO DE LEAD MOET NEMEN BIJ DE GDPR

exact.com/nl/gdpr

= exact

INHOUD

INTRODUCTIE

In veel bedrijven wordt gedacht dat voldoen aan de GDPR/AVG vooral een zaak voor de IT-afdeling en Legal is. Dat zijn immers de bedrijfsonderdelen die zich bezighouden met informatiebeveiliging en privacy / bescherming van persoonsgegevens. In werkelijkheid zal elke afdeling met deze nieuwe EU-privacywetgeving te maken krijgen: van marketing en sales tot en met Legal, IT en Finance. Blijft de hamvraag: wie neemt de leiding om jouw organisatie in lijn met de GDPR te brengen?

De GDPR heeft impact op de hele onderneming, maar het dossier kan het beste door de Chief Financial Officer (CFO) worden gedragen. Bij hem komen immers alle elementen van de GDPR bij elkaar. De CFO heeft zijn eigen hoofdgebied, maar managet functioneel vaak andere deelgebieden zoals IT en Legal. IT heeft te maken met managementsystemen waarin alle persoonsgegevens worden opgeslagen. Legal gaat over alle juridische aspecten van de GDPR en dit is ook de afdeling waar soms een Functionaris voor de Gegevensbescherming (interne toezichthouder) is ondergebracht. De marketingafdeling verzamelt gegevens over klanten en prospects en werkt vaak met CRM systemen. Vaak start het proces in een HRM of CRM systeem, maar uiteindelijk leidt alles tot een financiële transactie. Het is voor Finance van belang te weten wat er uiteindelijk aan persoonsgegevens in de financiële administratie komt vanuit de verschillende systemen.

Je organisatie compliant laten zijn met de GDPR, is een intern project dat je niet moet onderschatten. Er komen veel regels bij kijken die allemaal geborgd moeten worden in processen en procedures, en er zitten veel risico's aan vast. Daarom kun je dit project het beste op C-level onderbrengen.

ÉÉN 'PRIVACYWET' IN DE HELE EU

Vanaf 25 mei 2018 krijgen alle landen in de Europese Unie dezelfde privacyregels: de General Data Protection Regulation (GDPR). In Nederland is deze wet ook bekend onder de naam Algemene Verordening Gegevensbescherming (AVG). De nieuwe EU-privacy verordening geldt vanaf 25 mei 2018. Deze verordening zal vanaf die datum ook gelden voor alle landen buiten de EU die zaken willen doen met één of meer landen van de Europese Unie. Elke lidstaat van de EU heeft een toezichthouder die controleert of organisaties zich aan de GDPR houden.

Nederland: https://autoriteitpersoonsgegevens.nl

ARGUMENT 1

COMPLIANCY EN RISKMANAGEMENT

LIGT BIJ CFO

De afgelopen tien jaar zijn de bedrijfsrisico's die van invloed zijn op strategie en resultaat, exponentieel toegenomen. Zowel in aantal als in soort. Digitale innovaties jagen de veranderingen in een steeds hoger tempo aan en de regelgeving waar je als bedrijf aan moet voldoen, wordt steeds uitgebreider. De CFO heeft een leidende rol bij het bepalen en uitvoeren van de strategie, evenals bij het beheer van risico's en financiën. Hij is immers goed gepositioneerd om de risico's binnen de organisatie te beoordelen, te beheren en te integreren in de bedrijfsstrategie. De basis van Risk Managent is dat processen helder zijn gedefinieerd en gedocumenteerd. En het is vervolgens van belang dat dit niet alleen in de ivoren toren ligt: het zou de kracht van de CFO en zijn team moeten zijn om Risk Management door te laten dringen tot alle lagen van de organisatie en te integreren in alle bedrijfsmatige processen. Er moet samenwerking worden gezocht met operationeel management, zodat er op alle niveaus een 'buy in' is.

Kortom: de CFO heeft de (eind)verantwoordelijkheid, maar omdat het hier om meer gaat dan financiële risico's zal hij zijn beleid breder door de organisatie moeten uitzetten.

ARGUMENT 2

DE BOETE IS EEN BEDREIGING VOOR DE FINANCIËLE STABILITEIT

Wanneer er persoonsgegevens worden verwerkt, moet je kunnen aantonen dat deze verwerking voldoet aan de basisprincipes van de GDPR. Dat betekent dat je volledig transparant moet zijn waarom je gegevens vastlegt en wat je ermee gaat doen. Maar ook waar gegevens staan, of je ze binnen 4 weken inzichtelijk kunt hebben en of de veiligheid van de gegevens in orde is. En dat binnen elk proces in je organisatie waar met persoonsgegevens wordt gewerkt en door elke werknemer die deze gegevens verwerkt. Heb je je zaken niet op orde dan kunnen de boetes in de miljoenen lopen. Dat is voor elke CFO natuurlijk een regelrechte nachtmerrie. Want hoe kun je forecasten en begroten, terwijl het GDPR duiveltje over je schouder meekijkt? Ga je geld voor dit risico reserveren en kun je dit überhaupt zonder dat het impact heeft op je bedrijfsvoering? Of ga je ervan uit 'dat het zo'n vaart niet zal lopen'? Hoe ga je dat financiële gat dan dichten, wanneer je wel op je vingers wordt getikt? En wat is de impact op het bedrijfsimago naast de financiële? Wat is het gevolg voor de toekomst en stabiliteit van je onderneming? Kortom, voorkomen is beter dan genezen en zorg ervoor dat GDPR getackeld wordt voor het een financieel issue is.

ARGUMENT 3

DE CFO MOET DE CYBERSECURITY-KLOOF DICHTEN

Bij veel bedrijven is de CFO de eindverantwoordelijke voor IT. Dat maakt hem de aangewezen persoon om een cruciale bijdrage te leveren aan de cybersecurity van de onderneming. Het risico op datalekken neemt exponentieel toe. Enerzijds door toepassingen in producten en het Internet of Things, anderzijds door bijvoorbeeld het grote aantal systemen waarmee werknemers werken. Zeker wanneer het gaat om legacy systemen die in eigen beheer staan, is er een verhoogd risico.

Lang niet alle bedreigingen waar bedrijven aan blootstaan worden opgemerkt en technische beveiligingshulpmiddelen zijn niet altijd toereikend. Veelal zijn processen rondom veiligheid van data niet op orde. Weet jij of er een policy is, dat werknemers elke twee maanden hun wachtwoord moeten vernieuwen? Zijn de rollen en rechten in de systemen waar je in werkt goed ingeregeld? Werk je met een twee stap verificatie in je software naast de standaard gebruikersnaam en wachtwoord? In het geval van cybersecurity zijn processen en technologie maar een onderdeel van het geheel. Uiteindelijk draait het om de bewustwording bij medewerkers.

Hoe groter de kloof tussen bedreigingen waarop wel of niet wordt geanticipeerd, hoe meer risico je loopt bij incidenten. Wanneer het misgaat, kan dat miljoenen kosten: denk aan verloren zaken, het repareren van de schade en dalende waarde van de aandelen. Vanwege de relatie tussen cyberrisico en financieel risico, zou de CFO vooraan moeten staan om van de veiligheid prioriteit één te maken en het als zijn verantwoordelijkheid te beschouwen. Te vaak wordt cyberveiligheid aan IT uitbesteed en zij hebben te weinig zicht op de belangrijkste assets van een onderneming om de beste beslissingen in het belang van het bedrijf te kunnen nemen. De crux is dus dat de CFO net als bij andere risico's voldoende inhoudelijk begrip moet hebben van wat er wordt beschermd, waartegen en wat wel en niet relevant is om zo het juiste budget voor de juiste maatregelen te alloceren.

ARGUMENT 4

DE CFO ZIET DE KANSEN

VAN DE GDPR

Een slimme CFO is niet alleen op tijd voorbereid op de GDPR, maar weet er ook de vruchten van te plukken. Voldoen aan de GDPR leidt immers tot betere processen, betere inzichten en uiteindelijk tot een betere organisatie.

Data behoort tot de meest waardevolle bezittingen en zijn de rode draad in een onderneming. Sommigen spreken zelfs van het nieuwe goud. Maar dat is het alleen als je van data waardevolle informatie kunt maken. Ben je in staat om verbanden te leggen, trends te analyseren en conclusies te trekken. En weet je dit vervolgens te vertalen in mogelijkheden om er waarde uit te halen voor je klanten? Genoeg, zijn data een van de assets die de meeste organisaties het slechtst beheren: inconsistent, ongestructureerd en soms zelfs ad hoc. Voor veel bedrijven is het al een grote uitdaging om individuele afdelingen of medewerkers hun eigen data te laten beheren. Het zou ondenkbaar zijn dat bedrijven op deze manier met hun productielijnen, producten of omzet omspringen. Waarom dan wel met data?

De basis in het voldoen aan de GDPR zijn heldere en inzichtelijke processen. Gegevens moeten in één bron in de onderneming beschikbaar zijn. En dat maakt de nieuwe wet tot een kans voor bedrijven die weten hoe ze die moeten pakken. Ontdek waar data worden vastgelegd, in welke bronnen en systemen, of het efficiënt gebeurd en of het waarde toevoegt in het proces. Het voldoen aan de GDPR is het ideale moment om je processen te optimaliseren en 'waste' te voorkomen. Data, het analyseren van cijfers en op basis daarvan strategische adviezen geven, zet de CFO in zijn kracht. GDPR: pluk er je vruchten van.

ARGUMENT 5

IS JE AFDELING ER KLAAR VOOR?

Financiële afdelingen moeten bijzonder waakzaam zijn in de naleving van de GDPR. Neem het voorbeeld van facturatie. Dat is een potentiele nachtmerrie. Op facturen en in systemen staan contactpersonen met hun gegevens. Hoe bepaal je daarvan de bewaartermijn, rekening houdend met de wettelijke termijn van 7 jaar? Welke persoonsgegevens moet je langdurig bewaren (denk aan bijvoorbeeld werknemerscontracten voor potentiele pensioendiscussies) en welke gegevens kunnen wel binnen het termijn van 7 jaar geanonimiseerd worden? En waar staan deze persoonsgegevens? Wie kunnen erbij en hoe voorkom je dat er iets anders mee gebeurt waar geen instemming voor is gegeven? Of nog een lastigere vraag, hoe ga je bij een contactpersoon die op facturen staat om met het recht om vergeten te worden?

Ondanks alle vragen die de GDPR opwerpt, biedt het de CFO ook kans om het totale functioneren van de organisatie te verbeteren. Denk daarbij aan het normaliseren van gegevens van verschillende soorten systemen en het verzamelen van al die gegevens op één locatie. Dat maakt het aanzienlijk gemakkelijker om deze data in te zien, te analyseren en om erover te rapporteren. Je kunt rapportage- en meldingssystemen implementeren die vanzelf een melding geven als er zich problemen voordoen. Ook beveiligingsrisico's kun je met geautomatiseerde systemen en processen beheren. Het automatiseren van belangrijke processen, zoals facturering en purchase to pay, gaat je helpen om de belasting op je afdeling lichter te maken. Handmatige handelingen maken plaats voor herhaalbare, geautomatiseerde systemen met audit trails van processen, en deze helpen je vervolgens weer om te blijven voldoen aan de GDPR. En zo behoed je jezelf voor een van de belangrijkste veiligheidsrisico's die er zijn: menselijke fouten. De GDPR leidt tot minimalisering van risico's, terwijl het je het vermogen om op tijd en accuraat te rapporteren vergroot. Met als resultaat: een betere operationele efficiëntie.

Voorbereiding op GDPR is een bedrijfsbrede verantwoordelijkheid. Het is aan de CFO om de GDPR-kar te trekken…

HOE KAN EXACT HELPEN?

Exact zal al zijn software zoveel mogelijk geschikt maken om volgens de GDPR te werken. Dat betekent dat Exact functionaliteiten zal inbouwen om het gemakkelijker te maken om te voldoen aan de eisen in de GDPR. Daarbij kun je denken aan de mogelijkheid om documenten te labellen, zodat je er bijvoorbeeld aan toe kunt voegen hoe lang je een document mag bewaren, en wie het wel of niet mag inzien. 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 EN ONZE PRODUCTEN?

- Ga dan naar exact.com/nl/gdpr
- Neem contact met ons op.

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