Wortell CEO Danny Burlage:

“Veel organisaties zijn grotendeels al GDPR-ready”

Nederland is hard bezig om alles op het gebied van privacy op orde te krijgen. Volgens Danny Burlage, oprichter en CEO van Wortell, loopt Nederland binnen Europa voorop wat dit betreft. “Wij zijn heel veilig als het gaat om werken met data.”

Wortell helpt haar klanten in de zorg en de financiële wereld bij het invoeren van Microsoft cloud-technologie. Concreet betekent dat het installeren, implementeren en inrichten van systemen als Office 365, Outlook of Exchange. Burlage vertelt over een recent bezoek aan een internationale organisatie, waar hard aan de GDPR-compliancy wordt gewerkt. “Dat bereiden ze voor met een grote consultancy-organisatie. Wij bekeken voor hen de Office 365- en Microsoft cloud-omgeving. Die software is al in verregaande mate GDPR-ready. De diverse voorzieningen in de online versies van Exhange, Sharepoint en Office 365 hoeven alleen nog maar te worden geconfigureerd. Uiteraard bevinden bedrijfsspecifieke systemen zoals een klantendatabase, of andere maatwerkoplossingen zich buiten deze scope. Maar met cloud-gebaseerde systemen voor documentmanagement, e-mail en communicatie hebben bedrijven alle tools in handen om ervoor te zorgen dat ze grotendeels GDPR-compliant zijn. Heel veel organisaties zijn dus, zonder dat ze het zelf weten, al erg ver in het voldoen aan de nieuwe privacywetgeving. Het configureren en instellen van deze applicaties kunnen ze zelf. Ook kunnen ze het overlaten aan derde partijen, zoals Wortell. Aangezien dit onze expertise is, kunnen wij dit proces aanmerkelijk gemakkelijker maken voor hen.”

Danny Burlage, oprichter en CEO van Wortell

Beschamend

Wie dus de kantoorautomatisering online heeft geregeld met Microsoft-producten, voldoet in de basis voor een belangrijk deel aan de regels en richtlijnen van GDPR. Daarnaast biedt Microsoft via haar partners tools aan waarmee organisaties een assessment kunnen doen op hun basisinfrastructuur. Daaruit leren ze wat ze op welke manier moeten configureren, en welke stappen ze moeten ondernemen om bijvoorbeeld voor documenten, e-mail, chats en portals GDPR-compliant te worden. Burlage benadrukt dat ook de technische voorzieningen, waarmee organisaties kunnen aantonen dat ze er alles aan doen om veilig te blijven, voor een belangrijk deel in de cloud al zijn geregeld: “Zolang de basisinfrastructuur maar in de cloud draait bij gerenommeerde partijen als Microsoft. Alleen moet je dan wel weten dat het er is en hoe je het moet aanzetten. Organisaties die dat niet weten, of niet vertrouwd zijn met het configureren van die systemen, schaffen software soms twee- of zelfs driedubbel aan. GDPR is hot en wordt niet zelden – mede door handige consultants – opgeblazen. Hun belang is om zoveel mogelijk uren te schrijven. Dergelijke beschamende praktijken zagen we ook tijdens het zogeheten millenniumprobleem, waar it-consultants goed aan hebben verdiend. De verhalen over wat er allemaal mis zou kunnen gaan, werden zodanig opgeblazen dat het leek alsof de wereld zou vergaan. Ook nu weer wordt er nodeloos veel angst gezaaid. Af en toe is het alsof de wereld met GDPR opnieuw vergaat, maar de wereld vergaat helemaal niet.”

Commercieel belang

Burlage brengt in herinnering dat de GDPR wetgeving betreft waar wij allemaal om hebben gevraagd, zodat onze privacygegevens niet misbruikt kunnen worden. “Zeker is dat groot, en ja, het is belangrijk dat bedrijven zich hierop voorbereiden. Met name bedrijven en instellingen die werken met persoonsgegevens zoals burger servicenummers, patiëntgegevens of SWIFT-codes, moeten aan strenge eisen voldoen. Maar af en toe klinkt het alsof er met deze verordening een soort van donkere zeis op ons afkomt. In mijn ogen hebben de dienstverleners die deze angst zaaien daar voornamelijk een commercieel belang bij. Want als ik de hele kwestie nuchter bekijk, is het leeuwendeel van de regels en richtlijnen van GDPR te ondervangen door cloud-gebaseerde software.”

“Er wordt nodeloos veel angst gezaaid”

Veel organisaties in de zorgsector, aan de cure-kant, implementeren momenteel cloud-oplossingen voor hun communicatie en documenten. Zo brengen de Academische Ziekenhuizen hun volledige e-mail en documentenverkeer onder in de cloud, wat andere ziekenhuizen zeker zal doen volgen. “Dat staat los van hun EPD’s, die veelal in EPIC of Chipsoft zitten”, aldus Burlage. “Maar ook die systemen hebben uiteraard hun eigen GDPR-maatregelen getroffen.”

Data Privacy Officer

De cloud-applicaties ondervangen uiteraard niet alle punten in de verordening. Daarom pleit Burlage ervoor een Data Privacy Officer aan te stellen. “Want”, zo vertelt hij, “het is buitengewoon belangrijk om de updates voor software die niet in de cloud draait, regelmatig uit te voeren. De updates van Chipsoft maken hun software weliswaar GDPR-ready, maar dan moeten ze uiteraard wel worden geïnstalleerd. De bedrijven die zijn getroffen door ransomware als Wannacry en Petya, hadden niet de moeite genomen regelmatig updates te installeren. Als ze dat wel hadden gedaan, waren dergelijke gijzelingen nooit gebeurd. Een andere taak voor een DPO is ervoor te zorgen dat medewerkers goed worden geïnstrueerd hoe om te gaan met privacygevoelige data. En dan is er nog de kwestie van klantdata in legacy-systemen, waarvoor eveneens extra voorzieningen moeten worden getroffen. Kortom, er zijn genoeg zaken die een DPO in de gaten moet houden. Maar los van deze randzaken binnen het kader van GDPR, hebben bedrijven over het algemeen al de juiste software in huis die alleen nog maar hoeft te worden geconfigureerd. Het spijtige is dat ze dit vaak zelf niet weten.”

In de praktijk

Volgens Burlage zijn de cloud-applicaties van gerenommeerde partijen goeddeels GDPR-ready. Het is voornamelijk een kwestie van alles goed instellen of configureren. “Je kunt bijvoorbeeld instellen dat je waarschuwingen krijgt”, vertelt hij, “als je op het punt staat iets te doen dat in strijd is met de GDPR-regelgeving. Wanneer ik dan in Outlook een e-mailbericht schrijf met een burger servicenummer erin of andere herkenbare cliëntgegevens, dan krijg ik voordat ik het verstuur een waarschuwing. Maar je kan het ook zo instellen dat privacy-schendende handelingen eenvoudigweg niet meer worden uitgevoerd. De software is zo intelligent dat het naast waarschuwingen of het blokkeren van handelingen, ook proactief kan werken. Wanneer iemand bijvoorbeeld een bestand maakt met daarin honderden BSN’s of bankrekeningnummers of SWIFT-codes, dan kan het systeem die gegevens automatisch voorzien van een encryptie wanneer het echt verzonden moet worden.”