Quality Networks
ontwerpt, bouwt, beheert en beveiligt bedrijfsnetwerken

Nieuwe Europese privacyverordening: dit betekent het voor uw organisatie

De brief met cliëntgegevens die naar het verkeerde adres is gegaan en door een ander persoon geopend aan de receptie wordt afgegeven. De informatie over een cliënt die u via WhatsApp per abuis naar een privé-contact stuurt in plaats van naar de bedoelde collega. Het bekende verhaal van de verloren USB-stick of laptop die uit de auto wordt gestolen. Stuk voor stuk voorbeelden van datalekken die vanaf 25 mei 2018 onder de Algemene Verordening Gegevensbescherming vallen. Met alle, niet te onderschatten (financiële) gevolgen van dien…

Het waarom van de nieuwe verordening

Deze Europese verordening vervangt de Wet bescherming persoonsgegevens. Concreet betekent het dat de regels rondom privacy, óók voor u als organisatie, stevig worden aangescherpt. Boetes kunnen oplopen tot maximaal 20 miljoen euro. Reden voor deze wetsaanpassing is een besluit van de Europese Commissie en het Europees Parlement: zij zijn van mening dat de huidige wetgeving niet langer aansluit op de constante veranderingen in de digitale wereld. Gegevensuitwisseling houdt namelijk niet op bij landsgrenzen. Daarnaast kunnen overheid en bedrijfsleven, dankzij nieuwe technologie, bij hun activiteiten meer dan ooit gebruik maken van persoonsgegevens. Mensen moeten er op kunnen vertrouwen dat bedrijven en overheden netjes met hun persoonsgegevens omgaan. Met de nieuwe regels ontstaat in de gehele Europese Unie een gelijk niveau van bescherming.

Wat is een datalek ook alweer precies?

Er is sprake van een datalek wanneer er een incident heeft plaatsgevonden waarbij persoonsgegevens mogelijk in handen zijn gekomen van anderen. Ook is er sprake van een lek als gegevens verloren zijn gegaan of wanneer er niet kan worden uitgesloten dat dit niet gebeurd is. Voorbeelden te over: in oktober vorig jaar gijzelden criminelen nog een dag lang de computers van een Nijmeegse tandartspraktijk, waarbij ze mogelijk patiëntgegevens buit maakten.

Dit vraagt de nieuwe verordening van u

U bent verplicht om nóg transparanter te zijn over de persoonsgegevens die u verwerkt. Bijvoorbeeld door duidelijk uit te leggen wat u met deze data doet, hoe én hoelang deze exact wordt bewaard en welke rechten de persoon in kwestie heeft. Ook dient u duidelijk te zijn over de mogelijkheid om een klacht bij de Autoriteit Persoonsgegevens in te dienen. U kunt er bijvoorbeeld voor kiezen om een privacy statement op uw website te plaatsen. Een model-statement dat aan de geldende eisen voldoet download u hier (wil je dat op de site opnemen?).

Zó richt u uw bedrijf goed in

De AVG dwingt bedrijven om kritisch naar hun mensen, processen en techniek te kijken. Als verwerkingsverantwoordelijke bent u daarom verplicht om zowel technische als organisatorische

beveiligingsmaatregelen te treffen om de persoonsgegevens waar u mee werkt, goed te beveiligen. Bij elke factuur, (nieuws)brief of e-mailbericht moet er kritisch worden nagedacht of de manier waarop dit gebeurt voldoet aan de zeer strenge regelgeving. Sluit daarom bijvoorbeeld aan bij goedgekeurde certificeringsmechanismen, zoals de NEN-normen. Ook het instellen van een security officer kan verplicht zijn wanneer u op grote schaal met privacygevoelige persoonsgegevens werkt of personen structureel observeert. Het is van belang te beseffen dat uw netwerkinfrastructuur, zoals een virusscanner, firewall en router voldoen aan de eisen die de AVG stelt. Evenals een onderzoek waaruit blijkt hoe persoonsgegevens binnen uw organisatie op dit moment worden beveiligd, welke afspraken gemaakt zijn met het personeel, het opstellen van een privacybeleid en het bijhouden van een verwerkingsregister waarin alle gegevensverwerkingen worden geregistreerd. Andere voorbeelden zijn het sluiten van verwerkersovereenkomsten wanneer u voor gegevensverwerking gebruik maakt van de diensten van derden, zoals bijvoorbeeld een softwareleverancier. Zo'n overeenkomst regelt dat u de derden erop wijst dat er zorgvuldig met persoonsgegevens moet worden omgegaan en dat men zich exact dient te houden aan de afspraken die u met de betrokkenen heeft gemaakt. Verder raadt de Autoriteit Persoonsgegevens (AP) organisaties aan om actief een Data Protection Impact Assessment (DPIA) uit te voeren, wat met een onderzoek de privacyrisico's in kaart brengt zodat deze vervolgens zoveel mogelijk beperkt kunnen worden. Ook dient u bij het bepalen van de middelen die u inzet voor gegevensverwerking vooraf al rekening te houden met het privacy-aspect. Bijvoorbeeld door het juiste softwarepakket te kiezen.

Véél, héél véél informatie...

We kunnen ons voorstellen dat het u duizelt: probeer deze nieuwe materie daarom vooral niet in uw eentje te behappen, maar neem contact op met partijen die u hierbij zinvol kunnen ondersteunen.

Kies voor rust en zekerheid met het AVG-Ontzorgpakket

We kunnen ons voorstellen dat u niet staat te springen om de zoveelste verplichte wettelijke wijziging door te voeren binnen uw bedrijf. Kies daarom voor het AVG Ontzorgpakket, waarin wij u alle zorg uit handen nemen als het gaat om het technisch beveiligen van uw werkomgeving. Wij leveren een complete technische netwerkoplossing die uw bedrijf op dat onderdeel AVG-proof maakt. Voorbeelden daarvan zijn de keuze voor de best passende hardware en software waarmee wij een goede beveiliging kunnen realiseren.

Uiteraard verzorgen we ook onmisbare punten als privacyreglementen en (verplichte) verwerkersovereenkomsten die u kant-en-klaar aan uw cliënten kunt overhandigen. We vullen het ontzorgpakket verder aan met duidelijke checklists, heldere stappenplannen én een team van specialisten dat u, desgewenst 24/7, met raad en daad terzijde staat. Ook verzorgen we indien gewenst een korte, krachtige workshop om uw medewerkers bewust te maken van de

risico's rondom privacy. Uit onderzoek blijkt ook dat, naast goede software de mens meegenomen moet worden in dit proces.

Wat u ook nog moet weten...

De AVG biedt op een aantal plaatsen ruimte om nationale keuzes te maken. Deze worden vastgelegd in de Uitvoeringswet. Op dit moment is de Uitvoeringswet in Nederland nog niet vastgesteld. Dat betekent dat er nog een aantal onduidelijkheden over de nieuwe wet. Zo is nog niet exact afgebakend wat gegevensverwerking op 'grote schaal' dan precies is, waardoor ook niet helder is bij welke eenheden er een security officer moet worden opgesteld binnen uw organisatie. Diezelfde onduidelijkheid geldt voor het genoemde DPIA-onderzoek, dat als onderzoek verplicht wordt gesteld wanneer er een hoog privacyrisico bestaat voor betrokkenen. Op dit moment is er bijvoorbeeld nog niet duidelijk wat er precies onder een hoog risico wordt verstaan.

Wat al wel duidelijk is dat voortaan alle datalekken geregistreerd moeten worden. Dit in tegenstelling tot de huidige privacywetgeving die voorschrijft dat u datalekken alleen hoeft bij te houden als ze ook gemeld moeten worden aan de Autoriteit Persoonsgegevens.

Neem contact op

Bel met 088-695500 of stuur een e-mail naar sales@qualitynetworks.nl We vertellen u graag mee over onze krachtige oplossing om uw bedrijf klaar voor AVG te maken, zodat u zich in plaats van met nieuwe privacyregelgeving, vooral bezig kunt houden met ondernemen.