JML ICT

Bescherm de privacy van uw klanten op weg naar compliance met Europese privacy-wetgeving

Whitepaper voor CIO's, business- en ICT-managers

Wat is privacy

Privacy is het recht om te bepalen wie welke informatie over ons te zien krijgt, zodat we ‘onbespied en onbewaakt’ door het leven kunnen. Of het nu gaat om telefoonnummers, IP-adressen of gegevens over ras, godsdienst of gezondheid, het zijn allemaal persoonsgegevens die iets over iemand zeggen en dus beschermd moeten worden. De ‘bescherming van de persoonlijke levenssfeer’ is zelfs in de Grondwet vastgelegd.

Toch staat privacy steeds vaker onder druk. De digitale transformatie heeft gezorgd voor enorme dataverzamelingen die worden geanalyseerd en geïnterpreteerd, zonder dat klanten, patiënten of burgers daar toestemming voor hebben gegeven. Wet- en regelgeving moet ervoor zorgen dat de privacy beschermd blijft.

Met de Algemene Verordening Gegevensbescherming zet de Europese wetgever een nieuwe stap in die privacybescherming. Aan organisaties die persoonsgegevens van Europese burgers verwerken vanaf 25 mei 2018 de taak om compliance aan te tonen met deze nieuwe regelgeving.

Over onze whitepapers

Wij hebben een whitepaper opgesteld waarin u onze visie terugvindt op actuele onderwerpen. Soms over ICT-thema’s, soms over thema’s die daaraan raken. Deze whitepapers maken we om onze ervaring en expertise met u te delen, om u te inspireren en te laten zien wat er anno nu allemaal mogelijk is. Bent u aan de hand hiervan geïnteresseerd geraakt in ons en onze diensten? Neem gerust contact op via www.jml.nl of bel 0314 820223.

Inhoud

Onze visie

Met de Algemene Verordening Gegevensbescherming (AVG) dwingt de Europese wetgever een verantwoorde omgang met persoonsgegevens af. De AVG zorgt echter ook voor de nodige uitdagingen. Zo moet u in veel gevallen alle verwerkingen van persoonsgegevens bijhouden, aanvullende beveiligingsmaatregelen treffen en op regelmatige basis 'Privacy Impact Assessments' uitvoeren. Organisaties die per 25 mei 2018 klaar willen zijn voor de nieuwe wet doen er verstandig aan om tijdig te starten met de voorbereidingen.

Privacy is onmisbaar

Het onderwerp 'digitale privacy' staat volop in de belangstelling. Bijna dagelijks is er wel een datalek in het nieuws. Dan gaat het bijvoorbeeld om diefstal van laptops met daarop medische data, personeelsgegevens die voor iedereen zichtbaar op het internet staan of verlies van USB-sticks met daarop privacygevoelige informatie over burgers.

De massale (media-)aandacht voor datalekken is niet onterecht: een datalek kan voor klanten, patiënten of burgers verstrekkende gevolgen hebben. Zo kunnen kwaadwillenden met de persoonsgegevens identiteits-fraude plegen en op kosten van het slachtoffer bijvoorbeeld bestellingen plaatsen. Hierbij is de pakkans klein, zodat de schuldige de dans vaak ontspringt en het slachtoffer met de schade blijft zitten. Bij een lek van 'bijzondere persoonsgegevens' die inzicht geven in bijvoorbeeld iemands gezondheid, geloofsovertuiging of seksuele voorkeur bestaat het risico op discriminatie of stigmatisering.

Privacy is onmisbaar voor het vertrouwen in de digitale samenleving. Organisaties die met persoonsgegevens werken, hebben de wettelijke verplichting om hier zorgvuldig mee om te gaan. Klanten, patiënten en burgers verwachten dit ook: het is een grondrecht om informatie die privé is ook privé te houden. Zij moeten erop kunnen vertrouwen dat de bescherming van hun privacy absolute prioriteit heeft. Organisaties die hier onzorgvuldig mee omspringen, lopen het risico het vertrouwen van klanten te verliezen.

Sancties en meldplicht

Privacybescherming is dan ook een onderwerp dat niet alleen leeft onder ICT'ers en juristen, maar in toenemende mate ook in directiekamers. Wet- en regelgeving zorgt ervoor dat privacybescherming een onderwerp is waar directies zelfs niet meer omheen kunnen. Een lek van persoonsgegevens bijvoorbeeld kan resulteren in een flinke reputatieschade. Op basis van de Wet bescherming persoonsgegevens (Wbp) kan de Autoriteit Persoonsgegevens bovendien stevige boetes opleggen als een organisatie een datalek verzwijgt of onvoldoende beschermende maatregelen heeft getroffen.

De Europese Algemene Verordening Gegevens-bescherming (AVG) – de Nederlandse benaming voor de General Data Protection Regulation (GDPR) – voorziet vanaf 25 mei 2018 in nog hogere boetes en een bredere toepassing. Zo kunnen de boetes bij het niet naleven van de wet in het ergste geval oplopen tot maximaal 20 miljoen euro of 4 procent van de wereldwijde jaaromzet.

De meldplicht datalekken is slechts een onderdeel van de AVG. De nieuwe wet voorziet ook in nieuwe rechten voor betrokkenen, en in een reeks verplichtingen voor organisaties die persoonsgegevens verwerken. Die rechten en plichten zorgen voor de nodige administratieve lasten en dwingen ook organisatorische en technische maatregelen af om persoonsgegevens te beschermen.

In deze whitepaper leest u hoe u zich voorbereidt op de AVG en de privacy van uw klanten en medewerkers optimaal beschermt.

Privacywetten worden strenger

De digitalisering heeft ervoor gezorgd dat data eenvoudiger worden opgeslagen, verwerkt en gedeeld en dat ze onderdeel zijn geworden van nieuwe verdienmodellen. Persoonsgegevens worden doorverkocht of op een andere manier te gelde gemaakt. De bescherming van privacygevoelige data is daardoor een grotere uitdaging geworden, zeker met de huidige privacywet die is gebaseerd op een richtlijn uit 1995. Met de AVG is bescherming van privacy weer helemaal bij de tijd. Wij kunnen u helpen bij het beschermen van die gegevens.

Datalekken aan de orde van de dag

Veel organisaties beschikken over persoonsgegevens en wisselen deze uit. Door de digitalisering vindt die uitwisseling op een steeds grotere schaal plaats. Helaas gaat het daarbij regelmatig mis, met name in de gezondheidszorg, de financiële dienstverlening en het openbaar bestuur. Een groot deel van de 5500 data-lekmeldingen die de Autoriteit Persoonsgegevens (AP) in 2016 ontving, was afkomstig uit deze sectoren.

Privacygevoelige gegevens komen volgens de toezichthouder meestal in vreemde handen door een verkeerd bezorgde brief, een e-mail aan de verkeerde ontvanger of door onvoldoende beveiliging van een klantportaal waardoor klanten elkaars gegevens kunnen zien. Ook komt het vaak voor dat bijvoorbeeld een USB-stick met persoonsgegevens kwijtraakt of een laptop wordt gestolen. Zo raakten verschillende zorginstellingen persoonsgegevens kwijt na diefstal van een laptop of verlies van een USB-stick. De betrokkenen blijven vervolgens achter in de angst dat die gegevens in verkeerde handen vallen. Wij kunnen u helpen data bij diefstal te laten verwijderen. Hiervoor dient vooraf door ons software geïnstalleerd te worden. Vraag naar de mogelijkheden.

Huidige wetgeving voldoet niet meer

Wet- en regelgeving moet bescherming bieden tegen onrechtmatig gebruik van persoonsgegevens. De belangrijkste spelregels voor de omgang met persoonsgegevens zijn in Nederland vastgelegd in de Wet bescherming persoonsgegevens (Wbp). Hierin staat bijvoorbeeld dat de verwerking van persoonsgegevens in overeenstemming met de wet en ‘behoorlijk en zorgvuldig’ moet zijn, dat het doel van de verwerking bekend moet zijn bij degene van wie de persoonsgegevens zijn en dat de verwerking op een passende manier moet worden beveiligd.

Hoewel de Wbp de AP middelen geeft om op te treden tegen privacyovertredingen, oogst de privacywet toch al heel wat jaren forse kritiek. Zo is de Wbp – evenals de privacywetten in de 27 andere EU-lidstaten – gebaseerd op een Europese richtlijn die stamt uit 1995. Het internet stond toen nog in de kinderschoenen.

De EU-lidstaten hebben bovendien allemaal hun eigen invulling gegeven aan de richtlijn en die is niet altijd even strikt. Dit biedt bijvoorbeeld Amerikaanse bedrijven mogelijkheden om zich in Europa te plooien naar de minst strenge privacywet of om in de voorwaarden het Amerikaans recht van toepassing te verklaren. Ook komt het voor dat internationaal opererende bedrijven te maken hebben met meerdere privacywetten en verschillende toezichthouders.

Harmonisering privacywetgeving

De in mei 2016 in werking getreden Algemene Verordening Gegevensbescherming maakt een einde aan de versnippering van de privacywetgeving in Europa en zorgt voor een betere bescherming van persoonsgegevens. Uitgangspunt is een ‘rechtmatige, behoorlijke en transparante’ verwerking van gegevens die direct of indirect kunnen leiden tot de identificatie van een natuurlijk persoon.

De AVG is rechtstreeks van toepassing in alle EU-lidstaten en vervangt met ingang van 25 mei 2018 de afzonderlijke nationale privacywetten zoals de Wbp. Dat betekent dat er vanaf die datum nog maar één privacywet geldt in de hele Europese Unie. Alle Europese toezichthouders krijgen bovendien dezelfde, stevige bevoegdheden.

Tot die tijd is er sprake van een transitieperiode waarin de Wbp nog geldt. Die biedt organisaties de gelegenheid om hun bedrijfsvoering in overeenstemming te brengen met de AVG. Vanaf de genoemde datum moeten organisaties volledig compliant zijn met de Europese Privacyverordening, of kunnen aantonen vooruitgang te boeken.

Impact op uw organisatie

De Europese Privacyverordening kent 98 nieuwe of aangescherpte regels, allemaal met als doel om bij organisaties een betere controle over privacygevoelige data af te dwingen. Zeker tien wijzigingen hebben een grote impact op uw bedrijfsvoering. In de praktijk zal het dan ook niet meevallen om op 25 mei 2018 volledig compliant te zijn met de AVG. Daarvoor is de impact van de nieuwe wetgeving te groot. Begin daarom op tijd met de voorbereidingen en zorg ervoor dat u in mei 2018 in ieder geval vorderingen kunt laten zien.

Vergeleken met de Wbp legt de AVG andere accenten, onder andere als het gaat om:

•het vragen van toestemming voor het verwerken van privacygevoelige informatie. Hierin is de AVG strikter dan de Wbp. Het verzoek moet 'specifiek en ondubbelzinnig' zijn en duidelijk maken voor welk doel de verwerking is. Zonder een expliciete en vrijwillig gegeven toestemming is geen enkele verwerking toegestaan. De organisatie moet de toestemming vervolgens vastleggen en bewaren. Het is verstandig om al tijdens de voorbereiding uit te zoeken op welke wijze uw organisatie toestemming vraagt, verkrijgt, vastlegt en bewaart.

•de rechten van de betrokkenen. De AVG geeft individuen uitgebreide rechten om bijvoorbeeld toegang te krijgen tot de eigen informatie, fouten te laten herstellen en data te laten verwijderen en vernietigen. Een organisatie die een verzoek tot vernietiging ontvangt, moet alle data in leesbare vorm overdragen en vervolgens volledig verwijderen. Breng daarom tijdig in kaart waar privacygevoelige data zich bevinden, of die data in leesbare vorm zijn over te dragen en of ze intern zijn te vernietigen. Zorg bovendien voor data-governance door data te identificeren en classificeren en goede afspraken te maken over het datamanagement.

•privacy by design en de Privacy Impact Assessment. De AVG dwingt 'privacy by default' en 'privacy by design' af. Bij de ontwikkeling van een nieuwe dienst of product moet vanaf het begin rekening worden gehouden met de bescherming van privacygevoelige informatie. Een belangrijk onderdeel hierbij is het uitvoeren van Privacy Impact Assessments (PIA's). Van iedere wijziging moet duidelijk zijn wat de impact is op de bescherming van persoonsgegevens. Organisaties moeten daarom een proces hebben voor het uitvoeren, controleren en borgen van PIA's.

•het hebben van inzicht in waar data zich bevinden. Zonder inzicht is het onmogelijk om data te beschermen. Organisaties moeten bovendien toezien op de juistheid van de beschikbare data – die mogen tijdens de verwerking niet worden gewijzigd. Het instellen van een strikt beleid ten aanzien van toegang tot data- bestanden, identitymanagement en security- en compliancemonitoring zijn bijvoorbeeld manieren om te achterhalen wie toegang heeft tot data en wanneer data mogelijk zijn gewijzigd.

•security awareness. De AVG gaat ervan uit dat alle 'stakeholders' en medewerkers zich ervan bewust zijn dat ze met privacygevoelige informatie werken en dat ze op de hoogte zijn van de impact van een datalek.

Bij het bepalen van een eventuele boete zal de Autoriteit Persoonsgegevens zeker ook de investeringen in security-awarenessprogramma's meewegen. Uiteraard weegt ook mee welke beveiligingsmaatregelen een organisatie heeft getroffen. De AVG gaat veel meer dan de Wbp in op het belang van informatiebeveiliging. De aangescherpte regels in de AVG dwingen organisaties vooral om een strakke 'workflow' te hanteren. Zo moet er in veel gevallen sprake zijn van toestemming voor een verwerking van persoonsgegevens, bij de betrokkenen moet duidelijk zijn welk doel de verwerking dient, er moet een controle zijn op de juistheid van de informatie en op een correcte invoer en er moet worden gecontroleerd dat gegevens tijdens de verwerking niet wijzigen.

‘Privacy moet het uitgangspunt zijn bij de ontwikkeling van nieuwe diensten of producten’

10 actiepunten: Deze stappen helpen u bij de naleving van de AVG:

1.Investeer in security-awarenessprogramma’s. Iedereen – van werkvloer tot management, en ook uw leveranciers – moet zich er bewust van zijn wat de impact is van het werken met privacygevoelige informatie. JML ICT kan u hierbij helpen.

2.Controleer beschikbare informatie op juistheid. Wordt u door een betrokkene gewezen op een fout, dan moeten ook organisaties waarmee u onjuiste persoonsgegevens heeft gedeeld hiervan op de hoogte zijn.

3.Kijk of communicatie met betrekking tot het opvragen van privacygevoelige informatie helder is. Voor de betrokkenen moet direct duidelijk zijn met welk doel informatie wordt opgevraagd.

4.Bereid u voor op de uitgebreidere rechten van het individu. Er moeten richtlijnen en procedures zijn om bijvoorbeeld te kunnen voldoen aan een verzoek om fouten te herstellen of informatie te verwijderen.

5.Richt procedures in voor het melden van een datalek, mocht u dit voor de huidige meldplicht datalekken nog niet hebben gedaan. Tref security- maatregelen om datalekken op te sporen, te onderzoeken en zo volledig mogelijk binnen de gestelde termijn te melden bij de privacy-toezichthouder.

6.Bereid procedures voor op de striktere regels die gelden ten aanzien van toegangsverzoeken tot informatie door consumenten.

7.Zorg ervoor dat de juridische grondslag voor het verwerken van persoonsgegevens eenduidig is vastgelegd. Die grondslag moet bij het opvragen van privacygevoelige informatie in een ‘privacy notice’ en eventueel in het privacybeleid worden toegelicht.

8.Verzeker uzelf ervan dat toestemmingsverzoeken voor de verwerking van privacygevoelige informatie specifiek en ondubbelzinnig zijn. Betrokkenen moeten met een ‘duidelijke actieve handeling’ en op vrijwillige basis toestemming geven voor de verwerking van persoonsgegevens. Om privacy- gevoelige informatie van minderjarigen te mogen verwerken, moet een ouder of voogd toestemming geven. De toestemming moet controleerbaar zijn en in kindvriendelijke taal geschreven zijn.

9.Pas privacy by design toe en neem hierin Privacy Impact Assessments (PIA’s) op. Privacy moet het uitgangspunt zijn bij de ontwikkeling van nieuwe diensten of producten. Bij iedere wijziging is een PIA noodzakelijk.

10.Controleer of de aanstelling van een Data Protection Officer (DPO) noodzakelijk is. Overheids-instanties, bedrijven die het observeren van personen als kernactiviteiten hebben en organisaties die jaarlijks meer dan 5000 verwerkingen van privacygevoelige informatie uitvoeren, moeten zo’n ‘Functionaris Gegevens- bescherming’ in dienst hebben. De DPO houdt toezicht op de naleving van de AVG.

Op weg naar AVG-compliance

Compliance met de AVG vraagt om een gedegen voorbereiding waarmee u niet vroeg genoeg kunt beginnen. Zo moet u technische maatregelen treffen om persoonsgegevens te beschermen en de juiste processen inrichten voor bijvoorbeeld het vastleggen van dataverwerkingen en het uitvoeren van Privacy Impact Assessments. Ook moet u iedereen binnen de organisatie wijzen op het belang van privacybescherming en de eisen die de AVG daaraan stelt.

Tijdens de voorbereiding worden organisaties onder andere geconfronteerd met de volgende stappen:

1. Breng de huidige situatie in kaart

De voorbereiding op de AVG begint bij het in kaart brengen van de huidige situatie. Waar staat uw organisatie nu en welke aanvullende maatregelen zijn nodig voor compliance met de AVG? Is uw huidige registratie van gegevensverwerkingen voldoende? Heeft u een DPO nodig? En volstaat het privacybeleid nog? Om dergelijke vragen te beantwoorden, is het goed om de gereedheid (en hiaten) op de belangrijke aandachtspunten inzichtelijk te maken.

2. Breng persoonsgegevens en verwerkingen in kaart

Data kunt u pas beschermen als u weet waar ze zijn. Ook een verzoek tot vernietiging kunt u pas inwilligen als u weet waar de persoonsgegevens zijn opgeslagen. Ga na of de bestaande verwerkingen van persoonsgegevens zijn gedocumenteerd, en of die documentatie dan conform de AVG is. Kijk hierbij ook naar de overeenkomsten die u heeft met partijen die namens u persoonsgegevens verwerken. Volgens de AVG zijn alle partijen verantwoordelijk voor de bescherming van persoonsgegevens, dus zowel de organisatie die de persoonsgegevens verzamelt als de ‘externe verwerker’.

3. Voer een Privacy Impact Assessment uit

Hiermee brengt u de risico’s van de verwerking van de betrokken persoonsgegevens goed in kaart. Hierdoor ontstaat een beeld van de beschermende maatregelen die nodig zijn. Ook bij de ontwikkeling van een nieuw systeem of applicatie moet bij iedere wijziging een PIA worden uitgevoerd. De verbeteringen die u vervolgens aanbrengt op basis van de vastgestelde risico’s moeten worden gecontroleerd voordat een systeem of tool live gaat.

‘Het op orde hebben van de beveiliging is de basis om datalekken te voorkomen’

4. Tref beschermende maatregelen

Het op orde hebben van de beveiliging is de basis om datalekken te voorkomen. Dan gaat het om het implementeren van zowel organisatorische als technologische maatregelen. Daarbij kunt u denken aan het beveiligen van persoonsgegevens op mobiele devices met behulp van een Enterprise Mobility Management (EMM)-oplossing, het continu monitoren van de netwerkinfrastructuur op nieuwe kwetsbaarheden en het inzetten van een firewall.

Continue en beheerde monitoring van uw ICT-infrastructuur en kritieke bedrijfsprocessen helpt om cyberaanvallen vroegtijdig te onderscheppen en datalekken te voorkomen. Een goed inzicht in wat er is gebeurd, komt vervolgens ook van pas bij het melden van een datalek. Met een goede logging kunt u de gebeurtenissen als het ware nog een keertje afspelen.

5. Bereid de organisatie voor op incidenten

Securityincidenten, datalekken en 'gewone' privacy-incidenten zijn nooit helemaal uit te sluiten. Het is dan zaak dat de organisatie adequaat reageert, zodat de omvang van een incident beperkt blijft. Ook moeten de procedures voor het melden van een datalek bij de AP helder zijn. Het is raadzaam alle procedures regelmatig te oefenen en te evalueren. Zo kunt u verbeterpunten tijdig implementeren en maakt u uw organisatie weerbaar tegen de impact van (cyber)incidenten.

6. Richt de juiste controlemechanismen in

Zorg ervoor dat u in control en compliant blijft door de beschermende maatregelen continu te toetsen en indien nodig aan te passen. Ook moet iedereen zich blijven houden aan de gestelde maatregelen en zich bewust blijven van de mogelijke risico's bij de omgang met persoonsgegevens.

7. Maak van privacy by design prioriteit

Veel onderdelen van de AVG komen ook weer terug in het component privacy by design. U treft al tijdens de ontwikkeling van producten en diensten privacy-verhogende maatregelen en verwerkt zo min mogelijk persoonsgegevens. Onderkent u de privacyrisico's van een product of dienst niet in een vroegtijdig stadium, maar pas als de ontwikkeling ervan al een eind gevorderd is? Dan is de kans groot dat noodzakelijke aanpassingen zeer tijdrovend en kostbaar zijn voor u.

Onze dienstverlening en privacy

Het bewaken van de vertrouwelijkheid van communicatie is al sinds 1997 het fundament van onze onderneming. Wij beveiligen naast uw ICT-infrastructuur ook uw (privacygevoelige) data, intellectueel eigendom, persoonlijke gegevens én uw reputatie. Onze klanten kunnen er altijd op rekenen dat privacy en veiligheid onze hoogste prioriteit hebben.

Om uw organisatie voor te bereiden op de AVG hanteren wij een Security check die wij u aanbieden, zodat u de status weet op het gebied van de AVG wetgeving en Veiligheidsstatus die uw netwerk en organisatie op ICT gebied heeft. Als securityspecialist bieden wij bovendien de technische maatregelen die nodig zijn om de privacy van uw klanten te beschermen.

Wij hopen en gaan er van uit dat de vertrouwens relatie met JML ICT van hoog niveau is. Wij zeggen wel eens "u zult ons meer moeten vertrouwen dan uw eigen accountant". Uw accountant ziet voornamelijk alleen de cijfers. Uw ICT partner beheerd al uw data. De gegevens van u die bij ons bekend zijn staan veilig en versleuteld opgeslagen.

JML ICT hanteert strenge richtlijnen ten opzichte van en ook samen met onze ICT partners zoals providers, leveranciers en datacentra in binnen en buitenland. Om deze richtlijnen te kunnen blijven hanteren doen wij ons uiterste best dit met de partijen af te stemmen. Wij raden u aan dit ook met uw partners af te stemmen.

Wij komen graag bij u langs om uw organisatie te adviseren en maatregelen te treffen gegevens te beschermen en procedures te beschrijven.