ICT Academy

Whitepaper

De Europese Privacy Verordening: ‘showstopper’ of ‘business enabler’?

www.iir.nl

De Europese Privacy Verordening: 'showstopper' of 'business enabler'?

WAAROM EEN EUROPESE VERORDENING?

De Richtlijn bescherming persoonsgegevens van 1995 (richtlijn 95/46/EG) was een mijlpaal in de geschiedenis van de dataprotectie, maar deze richtlijn werd vastgesteld toen het Internet nog in de kinderschoenen stond. Na de nodige wetevaluaties heeft de Europese Commissie geconstateerd dat de huidige richtlijn verouderd is. De in 1995 vastgestelde regels hebben geleid tot grote implementatieverschillen tussen de Lidstaten en zijn ook steeds moeilijker toe te passen op de sterk veranderde op het web georiënteerde samenleving. Dit leidt steeds meer tot rechtsonzekerheid, onnodige kosten en administratieve lasten. De Europese Commissie stelt daarom een nieuw regelgevend kader voor dat de rechten van individuen versterkt, de dimensie van de interne markt vergroot en toch ook administratieve lasten voor ondernemingen beperkt. Het nieuwe kader, gebaseerd op artikel 16 van het EU-Werkingsverdrag, bestaat uit een Europese Privacy Verordening (EPV) die richtlijn 95/46/EG vervangt en een algemeen EU-kader bevat voor de bescherming van persoonsgegevens.

Anders dan een richtlijn die in nationale wetgeving moet worden omgezet om te kunnen worden geïmplementeerd, heeft een verordening directe werking. Dat betekent dat de verordening niet eerst naar nationale wetgeving hoeft te worden omgezet om te worden geïmplementeerd. De in de verordening opgenomen vereisten en definities, gelden dan ook in alle Lidstaten op dezelfde wijze.

WAT ZIJN IN HET OOG SPRINGENDE NIEUWE AANDACHTSPUNTEN?

Versterking van de rechten van individuen geschiedt door een reeks nieuwe maatregelen. De Europese Commissie streeft onder meer de verbetering na van de mogelijkheden voor individuen om de controle te houden over hun persoonsgegevens. Dit doet zij door:

- te verzekeren dat toestemming voor de verwerking van persoonsgegevens expliciet en vrijwillig wordt gegeven;
- introductie van een effectief recht om vergeten te worden in een online omgeving. Dit houdt in dat gebruikers een recht hebben op volledige verwijdering van hun persoonsgegevens indien zij hun toestemming intrekken en er geen andere legitieme redenen zijn om de data te bewaren; een gemakkelijke toegang tot de eigen persoonsgegevens te verzekeren, alsmede een recht op 'dataportabiliteit' (de vrijheid om data van de ene naar de andere dienstverlener mee te nemen);
- versterking van het recht op informatie over de wijze waarop persoonsgegevens (met name van kinderen) worden verwerkt. Daarnaast zet de Europese Commissie in op verbetering van de mogelijkheden voor individuen om hun rechten uit te oefenen. Dit doet zij door: de onafhankelijkheid en bevoegdheden van nationale toezichthouders voor gegevensbescherming te versterken; de administratieve en juridische (rechts) middelen te verbeteren in gevallen van schending van gegevensbeschermingsrechten. Ook het vergroten van de databeveiliging is een belangrijk streven van de Europese Commissie. Dit doet zij door: het gebruik van 'privacy enhancing' technologieën, van privacy vriendelijke standaardinstellingen en van programma's van privacy certificaten aan te moedigen;
- een algemene verplichting in te voeren om zogenaamde datalekken onverwijld te melden bij de toezichthouder en bij de betrokken individuen. Een ander belangrijk aspect van de Commissieplannen is vergroting van de verantwoordelijkheid van degenen die data verwerken. Dit geschiedt door: een verplichte functionaris voor gegevensbescherming (FG of Data Protection Officer / Privacy Officer) in bepaalde grotere bedrijven of bedrijven die aan 'risky processing' doen;
- introductie van het 'privacy by design' principe;
- een verplichting voor bedrijven die betrokken zijn bij 'risky processing' om een Privacy Impact Assessment (PIA) uit te voeren.

Een andere belangrijke nieuwe ontwikkeling is de invoering van een algemene en forse boetebevoegdheid. In de huidige wetgeving is een kleine boete alleen mogelijk voor overtreding van de (formele) meldingsplicht en niet voor een overtreding van de wet zelf. Met de EPV wordt een boetebevoegdheid ingevoerd waarmee boetes kunnen oplopen tot 100 miljoen euro of 5% van de wereldwijde jaaromzet.

MOGELIJKE SHOWSTOPPERS?

De belangrijkste mogelijke showstoppers zijn toch wel de verplichte aanstelling van een privacy officer, de meldplicht datalekken, het verplicht uitvoeren van privacy impact assessments op gevoelige verwerkingen en de invoering van het 'privacy by design' principe.

Een verplichte privacy officer is een wezenlijke verandering ten opzicht van de huidige situatie waarin een privacy officer nog vrijblijvend kan worden benoemd. Organisaties zullen dan ook expliciet moeten maken dat zij privacy als een risico zien dat door een speciaal daartoe benoemde persoon dient

te worden gemitigeerd. Vooral voor kleinere organisaties die gevoelige informatie verwerken, kan dit betekenen dat een privacy officer niet altijd binnen de eigen organisatie kan worden gevonden of benoemd en dat organisaties zich dan ook tot externe privacy adviseurs dienen te richten die op basis van inhuur de rol van privacy officer zullen gaan vervullen.

De meldplicht van datalekken is voer voor juristen. Het zal hier gaan draaien om definities. Definities die bij een onjuiste of onzorgvuldige inschatting door organisaties, kunnen leiden tot verregaande toezichtmaatregelen. Als er sprake is van een datalek (systeeminbraak door hackers maar bijvoorbeeld ook het verlies van een USB-stick met daarop alle financiële klantgegevens van een organisatie) dienen zowel de toezichthouder als de personen wiens klantgegevens zijn 'gelekt' zo spoedig mogelijk te worden geïnformeerd over het (al dan niet tijdelijke) verlies van de data. Dat vergt van organisaties dat zij steeds voorbereid, paraat en waakzaam zijn op het tijdig signaleren van een datalek en het treffen van de juiste en toereikende tegenmaatregelen.

Het uitvoeren van een PIA is een nieuwe ontwikkeling die de gegevensbescherming met grote sprongen tegelijk het pad der volwassenheid zal opsturen. Het opzetten en inregelen van een impact assessment is meestal specialistenwerk voor risk of audit managers. Niet elke privacy officer zal echter deze achtergrond hebben en deze persoon zal zich dan ook actief moeten gaan bemoeien met het juist en tijdig laten uitvoeren van deze assessments. De perfecte PIA bestaat niet: een PIA is namelijk altijd maatwerk. Afhankelijk van de mate van volwassenheid van een organisatie ten aanzien van risicobeheersing, zal dit evenzeer gelden voor de PIA. En ook een PIA in zich zelf beschouwd, is een lerend en levend instrument dat steeds in ontwikkeling is via de Plan-Do-Check-Act Cyclus.

Privacy by design houdt in dat als organisaties al tijdens de ontwikkeling van producten en diensten (zoals informatiesystemen) aandacht besteden aan privacyverhogende maatregelen, ook wel privacy enhancing technologies (PET) genoemd. Daarnaast dienen organisaties rekening te houden met dataminimalisatie: het zo min mogelijk verwerken van persoonsgegevens, dat wil zeggen alleen de gegevens die noodzakelijk zijn voor het doel van de verwerking. Op deze manier kan een organisatie zorgvuldige en verantwoorde omgang met persoonsgegevens technisch afdwingen. Privacy by design is echter geen sinecure. Het vergt commitment en doorzettingsvermogen van organisaties om dit principe op een adequate wijze te implementeren. Commitment omdat een organisatie zich er steeds van bewust dient te zijn dat nieuwe ICT applicaties een privacy impact kunnen hebben en dus in de ontwerpfase gechallenged moeten worden op de mate van bescherming van persoonsgegevens. Doorzettingsvermogen om de impact van privacy by design tot in detail te begrijpen en dit in de lange termijn planningen van de ICT-afdelingen ingebed te krijgen. Veel ICT-budgetten of ICT-systemen liggen immers al of voor lang vast.

MOGELIJKE BUSINESS ENABLERS?

Nieuwe regels betekenen veranderingen. De kernbeginselen van het privacyrecht wijzigen echter niet met de EPV. Denk dan aan principes als doelbinding, data-minimalisatie, beperkte bewaarduur, het vereiste dat gegevens juist en relevant zijn en dat gegevens eerlijk en rechtmatig moeten worden verwerkt. De gezamenlijke toezichthouders hebben enkele jaren terug aangekondigd dat ze 'accountability' een belangrijk principe vinden (dus dat organisaties kunnen uitleggen wat zij hebben gedaan om aan de privacywetgeving te voldoen). Bij accountability draait het eerder om het voldoen aan de kernbeginselen en de geest van het privacyrecht en aanzienlijk minder om de naleving en de handhaving van formele regels. Schending van een formele regel is in die visie dan minder ´erg´ als het niet voldoen aan een kernbeginsel.

Privacy by design en de verplichte privacy officer kunnen ook fungeren als business enabler. Door de vergrote aandacht voor de bescherming van persoonsgegevens, komt er ook meer aandacht voor informatiebeveiliging. Er is dan ook een grote overlap tussen de functies van (Information) Security Officer, Privacy Officer en de Compliance Officer. Dit vergt van de in toenemende mate complex en afhankelijk van ICT-systemen geworden organisaties, dat er een functionaris is die op alle terreinen kan schakelen. De functie van Privacy Officer zal in zwaarte en verantwoordelijkheid gaan toenemen. Dit zal het draagvlak en de importantie van de functie eveneens gaan vergroten. Met meer ervaring op privacy functies, zal ook het inzicht in de (on)mogelijkheden tot verandering van organisaties gaan verbeteren.

Privacy by design kan, goed toegepast, organisaties op een slimme manier voorbereiden op toekomstige ontwikkelingen of situaties. Denk aan het voorbeeld waarin een betrokkene zijn inzagerecht wil uitoefenen. Als er maar enkele verzoeken per jaar bij een organisatie binnenkomen, dan kan dit nog prima handmatig worden opgelost. Maar als de stroom inzageverzoeken zou gaan toenemen, leidt al dat handwerk tot hoge kosten. Als de ICT-applicaties al vanaf het ontwerp gebouwd zijn met inachtneming van het recht op inzage, kan dit er toe leiden dat de verzameling van persoonsgegevens die moeten worden verzameld en overgelegd aan de betrokkene, gestandaardiseerd, geautomatiseerd en dus veel sneller én goedkoper kunnen worden afgewikkeld. Een slim ICT-ontwerp kan dus in potentie veel kostenderving voorkomen.

WAT IS CONCREET DE IMPACT VAN DE EPV OP ORGANISATIES?

De EPV zal met zich meebrengen dat de EPV niet alleen juridisch moeten voldoen, maar ook materieel, dus dat de ICT-systemen er ook naar ingericht zijn én werken. Om dat te realiseren is een bijbehorend gedrag binnen een organisatie nodig dat hiermee in de pas loopt.

Concentreren op de huidige letterlijke tekst van de EPV is nog niet aan te raden. Zolang de tekst nog niet definitief vaststaat, kan er dus nog van alles veranderen. Dat betekent echter niet dat u achterover kunt leunen tot de helderheid over de toekomst van het privacyrecht er wel is. Er is immers nu ook al privacywetgeving. Deze is in Nederland voornamelijk vastgelegd in de Wet bescherming persoonsgegevens (Wbp) en deze wet zal in 2015 gaan veranderen als gevolg van een Nederlandse Wet meldplicht datalekken. De Nederlandse wetgever heeft er namelijk voor gekozen om vooruitlopend op de EPV, ook in Nederland al een meldplicht datalekken én een algemene boetebevoegdheid voor overtreding van de Wbp in het leven te roepen. Weliswaar is de boete niet zo hoog als die van de EPV ('slechts' maximaal 810.000 euro) maar dat betekent nog niet dat een dergelijke boete door organisaties snel als een 'geaccepteerd restrisico' zullen worden beschouwd.

Een organisatie verander je niet met een wet en ook niet over een nacht ijs. Veranderen van organisaties, zowel in ICT-architectuur als in gedrag van medewerkers, vergt regie en tijd. Tijd die tot aan de definitieve inwerkingtreding van de EPV, nuttig besteed kan worden aan een gedegen en structureel ingebedde verandering. Mits uit de impact assessments uiteraard is gebleken dat die verandering inderdaad noodzakelijk is…

LESSONS TO LEARN

De praktijktraining Introductie (EU) Privacy Regelgeving behandelt alle relevante aspecten van de EPV en de actuele wetsontwikkelingen in Nederland. Casusposities en dagelijkse situaties worden besproken aan de hand waarvan begrip van het regelgevend kader wordt gecreëerd. De nieuwe ontwikkelingen worden duidelijk afgezet tegen de huidige wetgeving in Nederland waardoor de training een ideale inleiding is voor medewerkers die zich voorbereiden op een nieuwe rol als privacy officer of voor diegenen die toe zijn aan een opfrissing van hun kennis.

mr. J.P. van Schoonhoven
Directeur adviesbureau Legal2Practice

Docent praktijktraining:
Privacy Officer 2.0
Privacy Audit Fundamentals
Introductie (EU) Privacy Regelgeving