Privacy en de Europese regelgeving

Er komt steeds meer aandacht voor het beschermen van privacy in de digitale wereld. En dat is maar goed ook, want bij het ontwerpen en bouwen van IT-systemen hebben vaak andere dingen voorop gestaan dan de bescherming van persoonsgegevens en de naleving van de wettelijke regels daaromtrent. De regels waren aanvankelijk ook weinig concreet, wat de implementatie – en het toezicht daarop door het College bescherming persoonsgegevens (CBP) – lastig maakte. Daarnaast had het CBP weliswaar ruime onderzoeksbevoegdheden, maar kon deze slechts beperkt sancties opleggen. Inmiddels zijn veel van de open normen verder uitgekristalliseerd. Het CBP heeft in de loop der tijd een reeks algemene richtsnoeren gepubliceerd.

Daarnaast wordt binnen afzienbare termijn de nieuwe Europese Algemene verordening gegevensbescherming (Avg) van kracht. Hoe de definitieve tekst eruit komt te zien wordt medio 2016, onder Nederlands voorzitterschap, pas duidelijk. Maar nu al weten we dat organisaties mechanismen moeten implementeren die er standaard voor zorgen dat wordt voldaan aan de privacyprincipes ('Privacy by Default'). Dit betekent dat privacybescherming al tijdens de systeemontwikkeling zal moeten worden meegenomen ('Privacy by Design', PbD).

De Europese verordening treedt twintig dagen na publicatie in werking. Naar verwachting wordt er een overgangstermijn van twee jaar in acht genomen. Dit betekent dat bedrijven en organisaties tot medio 2018 de tijd hebben om volledig te voldoen aan de AGV. Anders gezegd, bescherming van persoonsgegevens is een 'moving target' en elke organisatie die er mee te maken, heeft dient zijn kennis van tijd tot tijd te updaten.

Gastredacteur voor dit nummer is drs. Arjan Hassing RE RA (arjan.hassing@controlsolutions.nl). Hij is medeoprichter en partner van Control Solutions en gespecialiseerd in risk management, informatiebeveiliging en auditing. Daarnaast heeft hij een rol als 'teacher and revisor' bij de Universiteit Tilburg.

Forse uitbreiding boetebevoegdheid

Nieuwe m

dan met name op de komende wijziging daarvan. Daarnaast zijn meer specifieke en/of aanvullende regels te vinden in wetten als bijvoorbeeld de Wet politiegegevens, de Wet basisregistratie personen, de Telecommunicatiewet en de Wet geneeskundige behandelingsovereenkomst *(zie over laatstgenoemde de bijdrage van Peter Kits op pagina 26)*. Deze vallen buiten het kader van dit artikel.

Toepassingsbereik van de Wbp

De Wbp is gebaseerd op een Europese richtlijn uit 1995 en geldt in Nederland sinds 2001. Hij is van toepassing op de verwerking van persoonsgegevens in Nederland, en/of door of ten behoeve van een in Nederland gevestigde partij (ook al zou de eigenlijke verwerking in het buitenland plaatsvinden). Uitwisseling van persoonsgegevens met andere landen is slechts toegestaan indien het andere land een formeel erkend 'passend beschermingsniveau' voor persoonsgegevens kent. Binnen de EU is dat per definitie zo, omdat de nationale wetgeving overal op dezelfde Europese richtlijn is gebaseerd. Voor een beperkt aantal landen buiten de EU is vastgesteld dat ook die een passend beschermingsniveau hebben. Uitwisseling van persoonsgegevens met de rest van de wereld is in principe verboden, tenzij aan een reeks formele en praktische voorwaarden is voldaan (en soms is zelfs dat niet mogelijk).

De Wbp geeft zeer ruime wettelijke definities van de kernbegrippen 'persoonsgegeven' en 'verwerking'

Kernbegrippen

De Wbp geeft zeer ruime wettelijke definities van de kernbegrippen 'persoonsgegeven' en 'verwerking'. Daardoor zal er in bijna elk IT-systeem wel sprake zijn van verwerking van persoonsgegevens in de zin van de Wbp. Een persoonsgegeven is elk gegeven dat herleidbaar is tot een natuurlijk persoon (de betrokkene). Onder omstandigheden kan dat zelfs gelden voor gegevens die op het eerste gezicht behoorlijk anoniem lijken te zijn, zoals IP-adressen, kentekens, bankrekeningnummers en dergelijke.

Onder verwerking wordt vervolgens elke denkbare handeling verstaan die met (persoons)gegevens zou kunnen worden uitgevoerd, dus verzamelen, inzien, bewaren, kopiëren, verzenden, wissen, enzovoort.

Verder is van belang dat de verwerking van persoonsgegevens slechts is toegestaan als die is gebaseerd op een beperkt aantal wettelijke grondslagen. Bijvoorbeeld, als de verwerking noodzakelijk is voor de uitvoering van een overeenkomst met de betrokkene of als de betrokkene voor de verwerking zijn ondubbelzinnige toestemming heeft verleend. Bovendien mogen persoonsgegevens uitsluitend worden verzameld voor welbepaalde en gerechtvaardigde doeleinden, en de verdere verwerking moet ook steeds met de doeleinden verenigbaar zijn (doelbinding).

Tot slot kan in dit korte overzicht de beveiligingsplicht niet onvermeld blijven. Deze rust primair op de verantwoordelijke. Dat is degene die het doel van en de middelen voor de verwerking bepaalt. Elke organisatie die beschikt over bijvoorbeeld een personeelsadministratie, is ten aanzien daarvan de verantwoordelijke. Bij uitbesteding van (bijvoorbeeld) zo'n personeelsadministratie aan een bewerker moet de verantwoordelijke die plicht ook door middel van een schriftelijke bewerkersovereenkomst aan de bewerker opleggen. Het niveau van beveiliging moet volgens de wet passend zijn, gelet op de risico's die de verwerking en de aard van de te beschermen gegevens met zich meebrengen.

Naleving en toezicht

Bij het ontwerpen en bouwen van IT-systemen hebben vaak andere dingen voorop gestaan dan de bescherming van persoonsgegevens en de naleving van de wettelijke regels daaromtrent. Zie hierover de bijdrage van Jeroen van Puijenbroek *(pagina 35)*. De regels waren aanvankelijk ook weinig concreet, wat de implementatie – en het toezicht daarop door het CBP – lastig maakte. Daarnaast had het CBP weliswaar ruime onderzoeksbevoegdheden, maar kon deze slechts beperkt sancties opleggen. Inmiddels zijn veel van de open normen verder uitgekristalliseerd. Het CBP heeft in de loop der tijd een reeks algemene richtsnoeren gepubliceerd. Daarnaast heeft

het CBP aan de hand van een aantal incidenten rapporten gepubliceerd waarvan de conclusies ook voor andere organisaties toepasbaar zijn. Bovendien wordt met de komende wetswijziging het toezicht aanzienlijk verscherpt en zal het CBP (onder de nieuwe naam Autoriteit Persoonsgegevens) over geduchte sancties kunnen beschikken.

Meldplicht datalekken

De nieuwe meldplicht komt erop neer, dat de verantwoordelijke een logboek moet bijhouden van alle datalekken, dat hij van ernstige gevallen melding moet doen aan het CBP en soms ook aan alle personen van wie de gegevens (mogelijk) door het datalek zijn getroffen. Het niet voldoen aan de meldplicht kan leiden tot een hoge boete van het CBP.
Uiteraard is en blijft de eerste prioriteit het voorkómen van datalekken. Maar een datalek zit soms in een klein hoekje en dan is het goed om te weten wat er wanneer gemeld moet worden en aan wie. Dat maakt het mogelijk om de systemen en processen daar zo goed mogelijk op in te richten.

Meldplicht aan het CBP

De meldplicht aan het CBP geldt voor situaties waarin sprake is van een inbreuk op de beveiliging, die leidt tot 'ernstige nadelige gevolgen' voor de bescherming van persoonsgegevens of een aanzienlijke kans daarop. Een inbreuk is een doorbreking van de technische en organisatorische maatregelen die ter beveiliging van de persoonsgegevens zijn getroffen. De informatie die hierover aan het CBP moet worden gegeven omvat in elk geval de aard van de inbreuk, de instanties waar hierover meer informatie kan worden verkregen en de aanbevolen c.q. getroffen maatregelen om de negatieve gevolgen van de inbreuk te beperken.
Wanneer leidt een inbreuk nu tot (een aanzienlijke kans op) 'ernstige nadelige gevolgen'? Bij de beoordeling hiervan zijn volgens de wetgever een aantal aspecten van belang: (1) de aard en de omvang van het datalek; (2) de aard van de gelekte gegevens; (3) de mate waarin technische maatregelen zijn getroffen; en (4), de gevolgen van het datalek voor de persoonlijke levenssfeer van de getroffen personen. De verantwoordelijke moet per geval zelf een inschatting maken of een datalek wel of niet gemeld moet worden. Bij een hack zal dat bijvoorbeeld al snel het geval zijn. Bij de behandeling in de Tweede en Eerste Kamer zijn nog wat meer voorbeelden genoemd van meldplichtige datalekken, waaronder diefstal van laptops met gezondheidsgegevens van kinderen bij een gezondheidscentrum, het ongeoorloofd inzien van gegevens van verzekerden door een fout in een webapplicatie, een medewerker die zijn login-gegevens aan een derde geeft waardoor die bij duizenden klantgegevens kon komen en diefstal van een versleutelde, maar niet geback-upte laptop met hypotheekgegevens.
Er zijn echter maar weinig concrete voorbeelden gegeven van datalekken die niet gemeld zouden moeten worden. Dit blijft dus lastig. Het CBP heeft toegezegd de te maken afwegingen te zullen ondersteunen door het opstellen van richtsnoeren (beleidsregels) zodat bedrijven een duidelijk beeld hebben bij het maken van de afweging om

Bij het ontwerpen en bouwen van IT-systemen hebben vaak andere dingen voorop gestaan dan de bescherming van persoonsgegevens

een datalek wel of niet te melden. Ten aanzien van de inhoud van de melding en de wijze van melding zal aansluiting worden gezocht bij de reeds bestaande meldplicht op grond van de Telecommunicatiewet.
Naar verwachting zal het CBP deze richtsnoeren dit najaar ter consultatie aanbieden. Dat is dus een belangrijk moment voor bedrijven, brancheorganisaties en dergelijke om nog invloed te kunnen uitoefenen op de praktische invulling van de meldplicht.

Meldplicht aan de betrokkenen

In sommige gevallen moet een datalek behalve aan het CBP, ook aan de getroffen persoon of personen worden gemeld. Dit is het geval als de inbreuk "waarschijnlijk ongunstige gevolgen zal hebben voor diens persoonlijke levenssfeer". Het hoofddoel hiervan is, dat deze betrokkenen daarmee de kans wordt gegeven om extra maatregelen

te nemen om de mogelijk ongunstige gevolgen zoveel mogelijk te beperken. Bijvoorbeeld door het aanpassen van wachtwoorden, blokkeren van creditcards en dergelijke. Om die reden geldt er dan ook een uitzondering op deze meldplicht, als de getroffen gegevens adequaat versleuteld zijn, zodat deze voor derden onbegrijpelijk of ontoegankelijk blijven. Als het gaat om veel mensen (denk aan klanten-, abonneebestanden of een verenigingsadministratie), dan kan de meldplicht aan de betrokkenen een grote en ingewikkelde klus worden, die ook nog tot veel extra (negatieve) publiciteit kan leiden. Dat kan een extra reden zijn om gegevens standaard al te versleutelen.

Logboek

Tot slot zal de verantwoordelijke ook zelf een overzicht van alle ernstige datalekken moeten bijhouden. Het is de bedoeling dat de centrale beschikbaarheid van dit overzicht in een organisatie het zelflerend vermogen van die organisatie zal vergroten. Dit logboek bevat minimaal dezelfde feiten en gegevens als die aan het CBP en (indien van toepassing) aan de betrokkene moesten worden gemeld.

Het CBP zal veel hogere boetes kunnen opleggen voor bijna elke overtreding van de Wbp. De maximale boete bedraagt straks 810.000 euro

Rol van de bewerker

Als een organisatie de gegevensverwerking of delen daarvan heeft uitbesteed aan een externe bewerker, dan zal die organisatie voor de naleving van de meldplichten deels van die bewerker afhankelijk zijn. Als het goed is – zo staat dat immers ook al in de huidige wet – zijn de afspraken over de beveiliging al geregeld in een schriftelijke bewerkersovereenkomst. In de meeste gevallen zullen dergelijke bewerkersovereenkomsten dus moeten worden aangevuld met de nodige extra afspraken om aan de nieuwe meldplichten te kunnen voldoen. Van belang daarbij is ook de timing: bij ontdekking van een datalek moet dit namelijk 'onverwijld' worden gemeld. Dat betekent meestal binnen 24 uur. Om hieraan te kunnen voldoen zijn duidelijke afspraken nodig!

Uitbreiding boetebevoegdheden CBP

Naast de meldplicht voor datalekken betreft de tweede belangrijke wijziging van de Wbp een forse uitbreiding van de boetebevoegdheid van het CBP. De uitbreiding betreft zowel de mogelijkheid van het opleggen van boetes, als de hoogte van die boetes.

De huidige wetgeving biedt het CBP slechts beperkte mogelijkheden tot handhaving. Het CBP kan een bestuurlijke boete van maximaal 4.500 euro opleggen vanwege het niet-melden van verwerkingen van persoonsgegevens bij het CBP. Ook kan het CBP een soort dwangsom opleggen als een verantwoordelijke geen einde maakt aan een geconstateerde privacyschending (een 'last onder bestuursdwang'). Tot slot kan een strafrechtelijke boete worden opgelegd bij ongeoorloofd gegevensverkeer met derde landen. In de praktijk maakt het CBP vooral gebruik van publiciteit als effectief middel om overtreders aan te spreken. Maar ook de 'last onder dwangsom' wordt gebruikt: eind vorig jaar legde het CBP deze op aan Google vanwege het ontbreken van toestemming voor bepaalde verwerkingen en het niet-informeren van gebruikers. Die dwangsom kon oplopen tot 15 miljoen euro.

Door de wijzigingswet worden de boetebevoegdheden van het CBP in belangrijke mate uitgebreid. Het CBP zal veel hogere boetes kunnen opleggen voor bijna elke overtreding van de Wbp. De maximale boete bedraagt straks 810.000 euro of – als dat niet genoeg zou zijn – 10 procent van de jaaromzet van de overtreder. Bij opzet of ernstige verwijtbaarheid kan deze boete direct worden opgelegd; in andere gevallen eerst na schending van de door het CBP opgelegde 'bindende aanwijzing'. De bindende aanwijzing kan dus worden gezien als een gele kaart en de boete als de rode kaart. Daarnaast kan het CBP ook nog steeds gebruikmaken van de publiciteit (en van de last onder dwangsom).

De verwachting is dat het CBP (in lijn met het Autoriteit Consument en Markt) ook voor het opleggen van boetes richtsnoeren (beleidsregels)

zal opstellen en publiceren om zo meer duidelijkheid te verschaffen aan bedrijven.

Conclusie en aanbevelingen

Allereerst blijft het natuurlijk van het grootste belang om datalekken te voorkomen. Maar waar gehakt wordt vallen spaanders en dus moet een organisatie ook voorbereid zijn op het kunnen voldoen aan de nieuwe meldplicht. Gegeven de verwachte invoeringsdatum van 1 januari 2016 resteert hiervoor nu al minder dan een half jaar. Voor de IT-professional is van belang dat privacy nu nadrukkelijker dan ooit op de managementagenda zal moeten komen te staan en dat er concrete acties genomen moeten worden. Elke organisatie zal over een concreet en aantoonbaar privacybeleid moeten beschikken. Dit dient geïmplementeerd te zijn in haar processen en systemen. Daarnaast dienen medewerkers te zijn opgeleid om (mogelijke) privacygevoelige zaken te signaleren en op te pakken. Het is aan te bevelen om een duidelijk intern protocol in te voeren dat kan worden toegepast bij de ontdekking van een datalek.

Verder kan de wetswijziging aanleiding zijn om het bestaande beveiligingsbeleid (en de praktijk op dit punt!) nog eens kritisch te toetsen en, indien nodig, aan te passen. Zo kan worden overwogen om persoonsgegevens standaard te versleutelen teneinde de praktische en juridische (en publicitaire) gevolgen van een onverhoopt datalek te beperken. In veel gevallen zullen ook nadere afspraken met bewerkers moeten worden gemaakt over de beveiliging, en over de melding van datalekken. Deze afspraken dienen te zijn vastgelegd in bewerkersovereenkomsten. Het uitvoeren van Privacy Impact Assessments (PIA's) op processen en systemen zal hierbij een belangrijk hulpmiddel zijn. Zie hierover de bijdrage van Jeroen van Puijenbroek *(pagina 35)*.

Tot slot, als een organisatie kan aantonen steeds zoveel mogelijk de nodige zorgvuldigheid te hebben betracht bij de verwerking van persoonsgegevens, dan zal dat helpen als het eens zover komt dat het CBP aan de deur klopt. Hierbij is van belang dat een organisatie het CBP kan laten zien welke belangenafwegingen het heeft gemaakt en welke maatregelen er vervolgens zijn genomen. Op deze manier wordt het inzichtelijk voor het CBP en betrokkenen dat een organisatie 'privacybewust' handelt en zorgvuldigheid in acht neemt wanneer het gaat om persoonsgegevens. Zoals eerder gezegd vergt de implementatie van de nieuwe regelgeving de nodige energie, maar zo kan een organisatie het risico op een boete en publiciteit mitigeren en de schade aan de persoonlijke levenssfeer van de getroffen personen zoveel als mogelijk beperken.

mr. Rutger Alsbach (rutger@alsbach.nl) en mr. Saskia Sjardin (saskia.sjardin@capgemini.com) werken beiden als in-house counsel bij het Legal Department van Capgemini Benelux. Zij adviseren Capgemini op juridisch gebied over IT-services en gerelateerde juridische vraagstukken waaronder privacy. De auteurs hebben het artikel op persoonlijke titel geschreven.

Voor de IT-professional is van belang dat privacy nu nadrukkelijker dan ooit op de managementagenda zal moeten komen te staan

Literatuur

- Veel informatie is te vinden op de officiële site van het CBP: www.cbpweb.nl.
- De tekst van de Wbp staat op wetten.overheid.nl/BWBR0011468.
- De wijzigingswet van 4 juni 2015 staat hier (inclusief parlementaire geschiedenis): www.eerstekamer.nl/wetsvoorstel/33662_meldplicht_datalekken
- Bij de behandeling van het wetsvoorstel in de Eerste Kamer heeft de Staatssecretaris een buitengewoon handig overzicht gegeven van de huidige meldplichten die betrekking hebben op de bedrijfsvoering in de private of publieke sector. Dit is te vinden op: www.eerstekamer.nl/behandeling/20150519/memorie_van_antwoord_2/document3/f=/vju1h72cl3y5.pdf#12
- Om een idee te krijgen van de praktische invulling van de reeds bestaande meldplicht op grond van de Telecommunicatiewet, zie www.meldplichttelecomwet.nl