Bescherming van persoonsgegevens – een kwestie van vertrouwen

Privacy krijgt steeds meer aandacht in de samenleving. De Europese Unie is bezig met de Europese Privacy Verordening, die naar verwachting in 2015 in werking treedt. In dit artikel worden de belangrijkste gevolgen en de impact van de Verordening besproken.

Maurice Steffin - Risk Assurance, Assurance
Erica Zaaiman - New Technology & Security, Advisory
Adri de Bruijn - Technology, Advisory

1. Privacywetgeving steeds belangrijker

Privacy is een mensenrecht en staat als zodanig beschreven in de Universele verklaring van de rechten van de mens van de Verenigde Naties, het Handvest van de Grondrechten van de Europese Unie en de Nederlandse Grondwet. De EU-Richtlijn 95/46/EG heeft het recht op privacy verder uitgewerkt: natuurlijke personen moeten beschermd worden als het gaat om de verwerking van persoonsgegevens en het vrije verkeer van die gegevens. Deze richtlijn vormt de hoeksteen van het wetgevingskader voor de bescherming van persoonsgegevens van burgers in de EU.

De EU-lidstaten hebben EU-Richtlijn 95/46/EG geïmplementeerd in hun nationale wetgeving. In Nederland is de Richtlijn geïmplementeerd door middel van de Wet bescherming persoonsgegevens (Wbp). De Wbp stelt regels voor het verwerken van 'persoonsgegevens', ofwel gegevens betreffende een geïdentificeerde of identificeerbare natuurlijke persoon. De wet is van toepassing op zowel geautomatiseerde als niet-geautomatiseerde verwerkingen van persoonsgegevens die in een bestand zijn opgenomen. De Wbp is opgebouwd op basis van negen principes. Een van de principes is dat elke organisatie passende technische en organisatorische maatregelen treft om persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige verwerking.

In figuur 1 staat de tijdslijn van de wetgeving schematisch weergegeven.

Europese Privacy Verordening: meer vertrouwen in verwerking persoonsgegevens

Hoewel de principes en het kader van de Richtlijn nog steeds valide zijn is de implementatie in de nationale wetgevingen van de lidstaten binnen de EU op verschillende wijzen vormgegeven. Dit zorgt voor rechtsonzekerheid. Bovendien is in brede lagen van de bevolking het beeld ontstaan dat online activiteiten aanzienlijke risico's met zich meebrengen. Daarom heeft de Europese Unie het initiatief genomen voor de Europese Privacy Verordening. Deze zorgt voor een krachtig en coherent kader voor gegevensbescherming binnen de EU en een scherpe handhaving daarvan. Hierdoor kan de digitale economie zich op de hele interne markt ontwikkelen, kunnen burgers zelf bepalen wat er met hun gegevens gebeurt en is er meer rechtszekerheid voor bedrijven en overheden. De EU wil met deze Verordening het vertrouwen bij burgers en consumenten in de verwerking van persoonsgegevens door overheid en bedrijven vergroten.

De Europese Privacy Verordening is aangenomen door het Europees Parlement op 12 maart 2014. Als de Raad van Ministers met de Verordening instemt, treedt de Verordening per direct in werking voor alle lidstaten. Naar verwachting gebeurt dit in 2015 met een

Universele verklaring van de rechten van de mens, artikel 12 - Recht op eerbiediging van privé-, familie- en gezinsleven
"Een ieder heeft recht op respect voor zijn privé leven, zijn familie- en gezinsleven, zijn woning en zijn correspondentie. Dit houdt in dat er geen inmenging van enig openbaar gezag is toegestaan in de uitoefening van dit recht, dan voor zover bij de wet is voorzien en in een democratische samenleving noodzakelijk is in het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden of voor de bescherming van de rechten en vrijheden van anderen."

Handvest van de Grondrechten van de Europese Unie, artikel 7 – Eerbiediging van het privéleven en het familie- en gezinsleven
"Een ieder heeft recht op eerbiediging van zijn privéleven, zijn familie- en gezinsleven, zijn woning en zijn communicatie."

Handvest van de Grondrechten van de Europese Unie, artikel 8 – Bescherming van persoonsgegevens
"1. Een ieder heeft recht op bescherming van de hem betreffende persoonsgegevens.
2. Deze gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Eenieder heeft recht op toegang tot de over hem verzamelde gegevens en op rectificatie daarvan.
3. Een onafhankelijke autoriteit ziet toe op de naleving van deze regels."

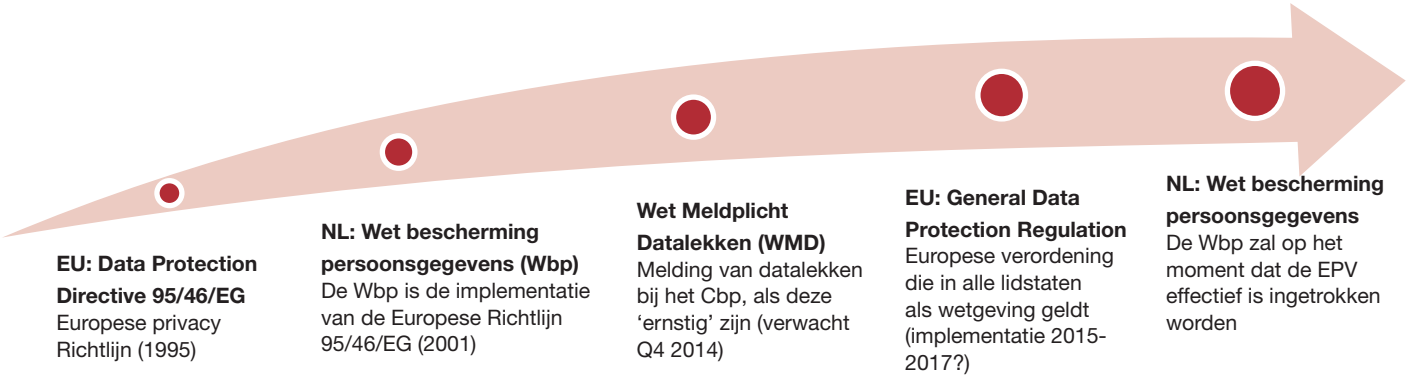
Grondwet, artikel 10 – Bescherming van persoonsgegevens
"1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.
2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.
3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens."

Samenvatting
De bescherming van persoonsgegevens speelt een steeds belangrijkere rol binnen organisaties. Technologische ontwikkelingen stellen organisaties in staat om meer en op uitgebreidere schaal persoonsgegevens te verzamelen, samen te voegen en op te slaan. Tegelijkertijd wordt de samenleving en de politiek kritischer hierover. De geplande invoering van de Europese Privacy Verordening is het Europese antwoord om het recht op privacy te beschermen en te verdedigen. De Verordening is opgebouwd rondom twee kernprincipes: 'Privacy by Design' en 'Privacy by Default'. In dit artikel worden de belangrijkste gevolgen en de impact van de Europese Privacy Verordening besproken.

implementatietermijn van twee jaar. De handhaving van de Verordening zal dan vanaf 2017 plaatsvinden.

Het vervolg van dit artikel is gebaseerd op de huidige versie van de Verordening, inclusief de amendementen van 12 maart 2014.

Figuur 1. Globale tijdslijn privacywetgeving



In voorbereiding op de aanstaande nieuwe Europese wetgeving heeft het Nederlandse kabinet het voorstel Wet Meldplicht Datalekken (WMD) ingediend. Het wetsvoorstel zoals het er nu ligt is niet helemaal in lijn met de Europese Privacy Verordening en daarom gaan er stemmen op om het voorstel terug te trekken of pas te behandelen nadat de Raad met de Verordening heeft ingestemd. Hieronder wordt ingegaan op de verschillen tussen de WMD ten opzichte van de Verordening.

2. Belangrijkste principes Europese Privacy Verordening: Privacy by Design en Privacy by Default

De twee belangrijkste principes van de Europese Privacy Verordening zijn:
- Privacy by Design; en
- Privacy by Default.

Privacy by Design gaat uit van het principe dat er in een vroeg stadium nagedacht wordt over:
- het goede gebruik van persoonsgegevens binnen een organisatie;
- de noodzaak van het gebruik van deze gegevens; en
- de bescherming ervan.

Door al bij het ontwikkelen van systemen de privacy en bescherming van persoonsgegevens in te bouwen is de kans op het succes ervan het grootst. Hoewel dit ook al ingebed is in de huidige Richtlijn, wordt met de komst van de Verordening meer nadruk gelegd op de daadwerkelijke uitvoering en handhaving.

Privacy by Default is een andere dimensie. Privacy by Default heeft betrekking op het toepassen van default settings op een zodanige wijze dat de privacy zo optimaal mogelijk wordt gewaarborgd.

Als onderdeel hiervan worden organisaties verplicht een intern privacy-beleid op te stellen, een functionaris voor de gegevensbescherming aan te stellen, privacy te integreren als vast onderwerp binnen de bedrijfsvoering, en de werking daarvan jaarlijks te controleren. Wanneer er veranderingen zijn in diensten en producten, processen en informatiesystemen, brengt de organisatie de consequenties en risico's gestructureerd in kaart op basis van een Privacy Impact Assessment (PIA). De Europese Privacy Verordening schrijft daarnaast een meldplicht voor bij inbreuken op persoonsgegevens.

Tevens krijgt de toezichthouder, in Nederland het College bescherming persoonsgegevens, meer bevoegdheden, waaronder de mogelijkheid tot het uitdelen van hoge boetes. In het vervolg van dit artikel gaan wij in op de vier belangrijkste wijzigingen, te weten de meldplicht voor inbreuken op persoonsgegevens, de versterking van de handhavingsbevoegdheden van toezichthouders, het verplicht aanstellen van een Functionaris Gegevensbescherming en het recht om te worden vergeten.

3. Inbreuk op persoonsgegevens moet tijdig gemeld worden

Een inbreuk op persoonsgegevens (datalek, privacy incident) moet door de verantwoordelijke organisatie binnen 24 uur nadat hij hiervan kennis heeft genomen, aan de toezichthouder gemeld worden. Ook moet de inbreuk, onder bepaalde voorwaarden, zo snel mogelijk na de melding bij de toezichthouder aan de betrokkene gemeld worden. Een van deze voorwaarden is dat de inbreuk waarschijnlijk negatieve gevolgen heeft voor de bescherming van de persoonsgegevens of de privacy van de betrokkene. Deze verplichting is van toepassing voor de verantwoordelijke organisatie, maar geldt ook voor de delen van zijn verwerking die hij uitbesteed heeft aan andere organisaties. Een voorbeeld hiervan is het uitbesteden van het beheer van een IT-omgeving of het call center. Treedt er bij de uitbestede verwerking (bij de opdrachtnemer) een datalek op, dan moet de verantwoordelijke organisatie dit ook tijdig melden.

Er is sprake van inbreuk als de technische en organisatorische beveiligings-maatregelen niet hebben gefunctioneerd en de persoonsgegevens blootgesteld zijn aan een aanmerkelijke kans op verlies of onrechtmatige verwerking. Dit hoeft niet automatisch te betekenen dat er sprake is van tekortschietende beveiligingsmaatregelen. Immers, men kan ook inbreken op een systeem als de beveiliging van voldoende niveau is. Echter, in situaties waarbij de inbreuk wel het gevolg is van een

Bezwaren Wet Meldplicht Datalekken

In het door het kabinet ingediende voorstel van de Wet Meldplicht Datalekken is in tegenstelling met de Europese Privacy Verordening de verplichting om inbreuken op persoonsgegevens te melden alleen opgenomen bij een als 'ernstig' te kwalificeren inbreuk. Dit geldt niet wanneer de verantwoordelijke organisatie 'passende' technische beschermingsmaatregelen heeft genomen waardoor de persoonsgegevens onbegrijpelijk of ontoegankelijk zijn voor derden. De organisatie zelf is verantwoordelijk voor het bepalen of er 'passende' technische beschermingsmaatregelen zijn genomen.

Door het toevoegen van het woordje 'ernstig' bij de meldingsplicht ontstaat er een verschil met de Europese Privacy Verordening zoals die nu is voorgelegd aan de Raad van Ministers. Dit is dan ook een van de bezwaren van het Cbp, voornamelijk doordat nog onduidelijk is wie bepaalt dat een datalek 'ernstig' is en wat 'ernstig' is.

De Wet Meldplicht Datalekken is momenteel in behandeling bij de Tweede Kamer.

tekortschietende beveiliging, kan dit de verantwoordelijke organisatie worden aangerekend. Bijvoorbeeld wanneer de verantwoordelijke organisatie slordig omgaat met wachtwoorden, e-mails met persoonsgegevens verkeerd adresseert, gevoelige stukken als oud papier aanbiedt, of een geheugenstick kwijtraakt.

De organisatie meldt in geval van inbreuk:
- de aard, omvang en schade van het datalek;
- de contactgegevens voor aanvullende informatie;
- aanbevelingen voor maatregelen om mogelijke nadelige gevolgen van het lek te verminderen;
- een omschrijving van de gevolgen; en
- een beschrijving van de inspanningen die de organisatie verricht om de inbreuk te herstellen.

De organisatie moet dus snel en effectief in kaart kunnen brengen:
- waar de inbreuk zich bevindt;
- welke bestanden worden geraakt; en
- wie geïnformeerd moet worden.

4. De Europese Privacy Verordening geeft handhavers meer bevoegdheden

Organisaties die de Verordening overtreden riskeren een hoge boete van maximaal vijf procent van de wereldwijde jaaromzet met een maximum van 100.000.000 euro. De eerste vraag die hierbij opkomt is: hoe kunnen organisaties dit voorkomen? Het meest simpele antwoord hierop is: door zich aan de wet te houden. In de wet staat namelijk precies wat een organisatie moet doen om persoonsgegevens voldoende te beschermen. De verwachting is dat als een organisatie kan aantonen dat zij de wet adequaat geïmplementeerd heeft en de principes uit de wet daadwerkelijk nageleefd heeft, dat niet overgegaan zal worden tot het opleggen van de maximale boete.

Het aantonen dat voldaan wordt aan de wet kan door middel van een goed privacy-governanceraamwerk waarin de risico's met bijbehorende beheersmaatregelen staan gedefinieerd. Aanvullende zekerheid kan hierbij gekregen worden door middel van interne en externe audits. In de Verordening is in dit kader ook het Privacy Protection Seal benoemd. Dit Privacy Protection Seal kan door een externe auditor afgegeven worden op basis van een privacy audit met een positief resultaat, waarmee naar de buitenwereld aangetoond kan worden dat de organisatie afdoende maatregelen heeft genomen om de bescherming van persoonsgegevens te waarborgen. De precieze invulling van dit Privacy Protection Seal is nog onderwerp van discussie. Overigens kent Nederland momenteel al een privacy-auditinstrument, het keurmerk Privacy-Audit-Proof. Dit keurmerk is ontwikkeld door beroepsorganisaties, en de Nederlandse toezichthouder heeft hiermee ingestemd. Op basis van een audit door een externe accountant of auditor met afdoende privacykennis kan een organisatie toestemming krijgen voor het voeren van dit keurmerk.

Het College bescherming persoonsgegevens (Cbp) heeft als nationale toezichthouder beperkte mogelijkheden voor het opleggen van boetes. Het College kan alleen een bestuurlijke boete opleggen van maximaal 4500 euro (art. 66 Wbp) voor het niet voldoen aan administratieve verplichtingen. Het Cbp is daarnaast gerechtigd om een last onder bestuursdwang of een last onder dwangsom op te leggen voor het niet voldoen aan de inhoudelijke bepalingen van de Wbp. Bij een last onder bestuursdwang of een last onder dwangsom heeft de organisatie eerst nog een beperkte periode om de overtreding van de Wbp te beëindigen. In dit geval wordt de last niet verbeurd.

Met de inwerkingtreding van de Europese Privacy Verordening krijgen de toezichthouders geharmoniseerde en krachtige handhavingsbevoegdheden, inclusief de hierboven beschreven boetebevoegdheid. De toezichthouder heeft het recht op informatie van bedrijven en organisaties en moet toegang kunnen krijgen tot hun panden. Tot slot krijgt het Cbp de bevoegdheid om een bedrijf in het uiterste geval stil te leggen, tot de organisatie zich wel houdt aan de geldende wetgeving.

5. Organisaties stellen verplicht een Functionaris Gegevensbescherming aan

Organisaties die meer dan 250 werknemers in dienst hebben, moeten een Functionaris Gegevensbescherming (FG) aanstellen. Een FG wordt benoemd voor een minimale periode van twee jaar. In zijn termijn geniet de FG ontslagbescherming. Een FG kan zowel een externe als een interne medewerker zijn, die specifieke kennis heeft van de geldende privacywetgeving, en hoe deze geïmplementeerd moet worden.

Het takenpakket van de FG omvat onder andere:
- de organisatie adviseren omtrent de Europese privacy-vereisten;
- de documentatie en procedures voor privacy-waarborging actueel houden;
- contact houden met het Cbp;
- eventuele datalekken monitoren en PIA's uitvoeren en monitoren.

6. Betrokkenen hebben het 'Recht om te worden vergeten'

Betrokkenen hebben het recht om van de verantwoordelijke te eisen dat alle persoonsgegevens van hem worden verwijderd. Dit 'Recht om te worden vergeten', of 'Right to be forgotten', is vooral van toepassing voor gegevens die door een betrokkene als kind ter beschikking gesteld zijn en op basis van enkele uitgewerkte gronden (Europese Privacy Verordening, art. 17). Dit geldt ook voor gegevens die met behulp van derden worden verwerkt en voor gegevens die openbaar gemaakt zijn. De focus van dit recht ligt voornamelijk op de zoekmachines waarin na jaren nog (vaak verouderde) informatie over personen is te vinden.

Op dit moment kent de Wbp het recht van verzet. Dit valt uiteen in twee vormen:

- ***Relatief verzet***
  Betrokkene kan bij bepaalde bijzondere persoonlijke omstandigheden verzet aantekenen tegen specifieke verwerking van gegevens.

- ***Absoluut verzet***
  Betrokkene wil niet dat zijn persoonsgegevens worden verwerkt in verband met de totstandbrenging of de instandhouding van een directe relatie tussen de verantwoordelijke en de betrokkene met het oog op commerciële doeleinden.

Voor beide gevallen van verzet geldt dat de betrokkene geen verzet kan aantekenen indien de verwerking plaatsvindt in het kader van een openbaar register dat bij wet is ingesteld, zoals de Basisregistratie Personen of het Basisregister Voertuigen.

Daarnaast geldt het recht om vergeten te worden niet indien dit in strijd is met het recht op vrijheid van meningsuiting, om redenen van algemeen belang op het gebied van de volksgezondheid, voor historische, statistische of wetenschappelijke doeleinden en ter voldoening aan een wettelijke verplichting tot bewaring van de persoonsgegevens op grond van EU-wetgeving of de wetgeving van de lidstaat waaraan de voor de verwerking verantwoordelijke onderworpen is. In de meeste gevallen zal in zo'n geval de verwerking van persoonsgegevens beperkt worden, waarna de gegevens alsnog na het aflopen van de bewaartermijn vernietigd worden.

7. Conclusie

Met de invoering van de Europese Privacy Verordening implementeren organisaties het 'privacy-denken' door middel van de twee achterliggende principes, Privacy by Design en Privacy by Default, om verlies van (persoons)gegevens, imagoschade en boetes te voorkomen. Dit betekent dat de organisatie een beleid moet uitstippelen over hoe om te gaan met persoonsgegevens. Ook brengt de organisatie in kaart waar de persoonsgegevens zich bevinden, hoe zij hiermee zal omgaan en welke bescherming van persoonsgegevens noodzakelijk is. Dit om te kunnen voldoen aan de Verordening en de Wet Meldplicht Datalekken. Daarnaast moet de organisatie aantoonbaar kunnen maken dat zij verantwoord omgaat met persoonsgegevens, bijvoorbeeld door een interne en/of externe privacy-audit, eventueel gecombineerd met het Privacy Protection Seal. Een sleutelrol bij bovenstaande is weggelegd voor de Functionaris Gegevensbescherming die dit proces zal begeleiden en monitoren.

Ondanks dat de Verordening nog niet definitief is en er waarschijnlijk een implementatietermijn van toepassing zal zijn van twee jaar, is het goed als organisaties alvast de gevolgen hiervan beoordelen, zodat zij de tijd hebben om zich voor te bereiden op de daadwerkelijke inwerkingtreding. Het implementeren van een adequate privacy governance is een continue investering, die zich enkel terug zal verdienen door het voorkomen van inbreuken op persoonsgegevens en daarmee het voorkomen van reputatieschade.