De nieuwe Europese Privacywetgeving

Paul Breitbarth

Director of EU Certification Research & Senior Solutions Advisor

NVRR Mini-Congres, 24 November 2017

NVRR
Nederlandse Vereniging van Rekenkamers & Rekenkamercommissies

NYMITY
innovating compliance

Wat is de Algemene Verordening Gegevensbescherming ?

NYMITY
innovating compliance

De nieuwe Europese Privacywetgeving

General Data Protection Regulation (GDPR) / Algemene Verordening Gegevensbescherming (AVG)

Verordening (EU) 2016/679

- Vervangt de bestaande Europese regels uit 1995 (pre-internet) en de Wet bescherming persoonsgegevens (2001)
- Creëert een gelijk speelveld voor de hele Europese Unie en zet nieuwe wereldwijde standaard voor gegevensbescherming
  - Uitwisseling gegevens binnen de EU is geen enkel probleem
  - Uitwisseling buiten de EU is aan strenge regels gebonden
- Geeft invulling aan de bescherming van de grondrechten op privacy en gegevensbescherming (voorheen m.n. regeling voor interne markt EU)
- Meer verantwoordelijkheid bij bedrijven, scherper toezicht, meer rechten burgers

De nieuwe Europese Privacywetgeving

Kernbegrippen van de wet

- Rechtmatigheid, behoorlijkheid en transparantie
- Doelbinding: verwerking voor vooraf bepaalde, helder gespecificeerde doeleinden; verdere verwerking van dezelfde gegevens alleen als dat verenigbaar is met het oorspronkelijke doel
- Gegevensminimalisatie (niet meer gegevens dan nodig) en juistheid van de gegevens
- Gegevensbeveiliging

Wat is een gegevenswerking ?

- Alles wat met persoonsgegevens wordt gedaan (verzamelen, bewaren, bewerken, archiveren, wissen, etc.)

De nieuwe Europese Privacywetgeving

Kernbegrippen van de wet

Wat is een persoonsgegeven ?

- Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon
- Identificeerbaar: direct of indirect, ook door combineren datasets
- Pseudoniem ≠ anoniem

Wat zijn bijzondere / gevoelige persoonsgegevens ?

- Gegevens over ras, etniciteit, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap vakbond, strafrechtelijk verleden, gezondheid en seksualiteit; genetische en biometrische gegevens;
- Alleen verwerken als dat expliciet in de wet is toegestaan (incl. wetenschappelijk onderzoek)

De nieuwe Europese Privacywetgeving

Toepassing van de wet

Wat valt onder de wet ?

- Alle verwerkingen door overheid en bedrijfsleven in de EU, of gericht op de EU
- Uitzondering: EU-instellingen en politie / justitie
- Uitzondering: elektronische communicatiediensten (ePrivacy), incl. cookies

Inwerkingtreding

- 25 mei 2016 – inwerkingtreding Algemene Verordening Gegevensbescherming
- 25 mei 2018 – alle bepalingen van de GDPR volledig van kracht
- Uitvoeringswet GDPR volgt nog op nationaal niveau (aanvulling op GDPR)
- Geen verder uitstel

Wat moet er gebeuren ?

NYMITY
innovating compliance

De nieuwe Europese Privacywetgeving

De basis voor elke gegevensverwerking

- Grondslag (1 van de 6 opties):
  - Toestemming
  - Uitvoering van een contract (en pre-contractuele fase)
  - Wettelijke verplichting
  - Vitaal belang van een individu
  - Publiek belang van de organisatie
  - Gerechtvaardigd belang van de verantwoordelijke
- Transparantie over gegevensverwerking
  - Wat is het doel van de verwerking?
  - Wie is de verantwoordelijke?
  - Waar gaan de gegevens heen?
  - Hoe lang worden ze bewaard?

Voorwaarden **toestemming**:
- Op basis van duidelijke en begrijpelijke informatie
- Vrijwillig gegeven
- Ondubbelzinnig

Gerechtvaardigd belang is een afweging van het economisch belang van het bedrijf vs. de grondrechten van het individu (niet alleen privacy!)

Bewaartermijnen:
- Niet langer dan noodzakelijk
- Liefst zo concreet mogelijk
- Anders criteria voor verwijdering

De nieuwe Europese Privacywetgeving

Verwerking van gegevens door Rekenkamers

Grondslag voor verwerking: Publiek Belang

Geregeld in artikel 183 Gemeentewet io. artikel 6(1) en onder e GDPR

- *De rekenkamer is bevoegd alle documenten die berusten bij het gemeentebestuur te onderzoeken voor zover zij dat ter vervulling van haar taak nodig acht.*
- *De verwerking is alleen rechtmatig indien en voor zover aan ten minste een van de onderstaande voorwaarden is voldaan;*
  - *de verwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de verwerkingsverantwoordelijke is opgedragen*

Maar: verwerkingsverbod bijzondere persoonsgegevens – toestemming vereist!

De nieuwe Europese Privacywetgeving

Verwerkersovereenkomsten

- Een verwerker is een persoon of organisatie aan wie de verantwoordelijke de gegevensverwerking heeft uitbesteed (bijvoorbeeld een administratiekantoor of een cloud service provider).
- Een verwerker handelt altijd namens de verantwoordelijke, en dient kaders mee te krijgen hoe hij gegevens mag verwerken. Dit wordt vastgelegd in een **verwerkersovereenkomst**. De overeenkomst bevat onder meer:
  - De details van de verantwoordelijke, de verwerker en de eventuele sub-verwerkers (en bepalingen over het toestaan van subverwerkingen)
  - De beveiligingseisen waar de verwerker aan moet voldoen
  - Bepalingen over het verwijderen van gegevens bij beëindiging van de overeenkomst
  - Bepalingen over de medewerking van de verwerker bij verzoeken om informatie van individuen of de toezichthouder

De nieuwe Europese Privacywetgeving

Meldplicht datalekken

- Een datalek moet zonder vertraging (zo mogelijk binnen 72 uur) worden gemeld aan de Autoriteit Persoonsgegevens, gerekend vanaf het moment dat het lek bekend is geworden in de organisatie
  - Uitzondering: als het onwaarschijnlijk is dat het lek een risico voor het individu heeft opgeleverd (bijvoorbeeld een koffer met dossiers die nog steeds op slot zit)
  - Meldplicht geldt zowel voor digitale als fysieke lekken, en ook als nog niet alle omstandigheden duidelijk zijn. Bij twijfel kan altijd pro forma worden gemeld, met een aanvulling op een later moment.
- Bij een hoog risico op nadelige gevolgen voor het individu moet het lek ook aan alle betrokkenen worden gemeld, tenzij de gegevens versleuteld zijn (encryptie) of meteen maatregelen zijn genomen om misbruik tegen te gaan.

De nieuwe Europese Privacywetgeving

De Functionaris voor Gegevensbeschermng

- Voor het eerst verplicht in de hele Europese Unie, wanneer:
  1. de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan
  2. de verwerkingsverantwoordelijke hoofdzakelijk is belast met verwerkingen die regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen
  3. de verwerkingsverantwoordelijke hoofdzakelijk is belast met verwerkingen van bijzondere persoonsgegevens
  - Criteria 2 and 3 zijn afhankelijk van grootschalige verwerkingen, op grond van het aantal betrokkenen, de hoeveelheid gegevens, de duur van de verwerking en de geografische reikwijdte
- FGs worden aangesteld op grond van hun professionele kwaliteiten en kundigheid
- FGs dienen naar behoren en tijdig worden betrokken
- FGs moeten toegang hebben tot de benodigde (*voldoende*) middelen
- Een FG mag geen instructies krijgen over de uitvoering van zijn taak

De nieuwe Europese Privacywetgeving

De Functionaris voor Gegevensbeschermng

Belangrijkste taak: toezien dat de GDPR wordt gerespecteerd

- Informatie verzamelen over de verwerkingen
- Analyse en rechtmatigheids-check van de verwerkingen
- Advies en aanbevelingen uitbrengen aan verantwoordelijke en verwerker
- Bijdragen aan de uitvoering van GEBs (PIAs)
- FGs zien zelf niet verantwoordelijk in geval van overtreding van de GDPR
- Belangrijkste contactpersoon voor de AP
- Activiteiten en inspanningen worden geprioriteerd obv risico (voor betrokkene)
- (evt.) Bijhouden van het verwerkings-register
- In de praktijk: Beleid ontwikkelingen voor bescherming persoonsgegevens

De nieuwe Europese Privacywetgeving

Accountability: de verantwoordingsplicht

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van lid 1 en kan deze **aantonen** („**verantwoordingsplicht**”).
Artikel 5(2) GDPR

Rekening houdend met de aard, de omvang, de context en het doel van de verwerking, alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, treft de verwerkingsverantwoordelijke **passende technische en organisatorische maatregelen** om te waarborgen en te kunnen **aantonen** dat de verwerking in overeenstemming met deze verordening wordt uitgevoerd. Die maatregelen worden **geëvalueerd** en indien nodig **geactualiseerd**.
Artikel 24(1) GDPR

De nieuwe Europese Privacywetgeving

Accountability: de verantwoordingsplicht

- De verantwoordingsplicht vereist dat u kunt aantonen wat u doet:
  - Aan de toezichthouder
  - Aan betrokkenen (klanten, medewerkers, etc.)
- Een andere aanpak van de toezichthouders: minder controles vooraf, meer achteraf.
- Helpt het risico op onderzoek en/of sancties te verkleinen
- Stelt organisaties in staat sneller te reageren op klachten of datalekken – spaart tijd
- Groot verschil tussen het kunnen voldoen aan de wet (momentopname) en het blijven voldoen aan de wet (in staat zijn om met veranderende omstandigheden op te gaan omdat de technische en organisatorische maatregelen goed zijn geïmplementeerd)
- **De verantwoordingsplicht vereist voortdurende aandacht**

De nieuwe Europese Privacywetgeving

Internationale uitwisseling van gegevens

- Binnen de Europese Unie zijn er geen beperkingen
- Buiten de Europese Unie mogen gegevens alleen worden doorgegeven naar landen met een passend beschermingsniveau
- Uitzonderingen:
  - Gebruik van modelcontracten of andere goedgekeurde bindende afsp
  - Bindende bedrijfsvoorschriften (Binding Corporate Rules) – alleen bin
  - Uitzonderingen in specifieke situaties (eenmalig): toestemming, uitvo vitaal belang, etc.

* https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensve buiten-de-eu#welke-modelcontracten-zijn-er-voor-doorgifte-naar-een-derde-land-55

- Andorra
- Argentinië
- Canada (private sector)
- Faeröer Eilanden
- Guernsey
- Isle of Man
- Israël
- Jersey
- Uruguay
- Verenigde Staten (Privacy Shield)
- Zwitserland

De nieuwe Europese Privacywetgeving

De toezichthouder - taken

- Monitoren en handhaven van de toepassing van de Verordening
- Bevorderen van de publieke bekendheid van de regels, waarborgen en rechten
- Informatie verstrekken aan betrokkenen over de uitoefening van hun rechten
- Klachten behandelen van individuen or organisaties en, voor zover mogelijk, de inhoud van de klacht onderzoeken
- Onderzoeken uitvoeren naar de toepassing van de wetgeving in de praktijk
- Verschillende administratieve taken, onder meer ten aanzien van internationale doorgifte, gedragscodes en certificering

De nieuwe Europese Privacywetgeving

De toezichthouder - bevoegdheden

- Alle informatie over gegevensverwerkingen kan door de Autoriteit Persoonsgegevens (AP) worden gevorderd, inclusief de gegevens zelf
- De AP heeft het recht alle gebouwen en kantoren van de verantwoordelijke te inspecteren, inclusief alle apparatuur
- De AP kan een waarschuwing afgeving als een verwerking in strijd dreigt te zijn met de wet
- De AP kan eisen dat een verwerking in overeenstemming wordt gebracht met de wet
- De AP kan de verwerking tijdelijk of definitief stilleggen
- De AP kan een boete opleggen: tot €20 miljoen, of 4% van de bruto jaaromzet

De nieuwe Europese Privacywetgeving

De toezichthouder – de leidende toezichthoudende autoriteit en het Comité

- Een van de grote veranderingen in de GDPR: verplichte internationale samenwerking tussen toezichthouders
- Nieuw concept: de leidende toezichthoudende autoriteit

De leidende toezichthoudende autoriteit: de toezichthoudende autoriteit van de hoofdvestiging of de enige vestiging van de verwerkingsverantwoordelijke of verwerker is bevoegd op te treden als leidende toezichthoudende autoriteit voor de grensoverschrijdende verwerking. Hij is voor de verwerkings-verantwoordelijke of de verwerker de enige gesprekspartner bij grensoverschrijdende verwerking.

- Platform voor afstemming en samenwerking: het Europees Comité voor Gegevensbescherming
  - EU orgaan met rechtspersoonlijkheid, bestaande uit vertegenwoordigers van de nationale toezichthouders en de EDPS
  - Permanente voorzitter, met een vast secretariaat in Brussel (bij de EDPS)
  - Opvolger van de Artikel 29 Werkgroep voor Gegevensbescherming
  - Zorgt ervoor dat de GDPR consequent wordt toegepast, met behulp van richtsnoeren, adviezen en opinies.

De nieuwe Europese Privacywetgeving

Het Coherentiemechanisme

- Elk besluit dat een gevolg kan hebben in meer dan één EU lidstaat, dient voor advies te worden voorgelegd aan het Comité voordat het definitief wordt vastgesteld. Op deze manier kan het Comité een consequente uitleg van de GDPR bevorderen.
- Elke toezichthoudende autoriteit, de voorzitter van het Comité of de Europese Commissie kan vragen om een onderwerk te laten bespreken door het Comité.
- Wanneer er tegenstrijdige zienswijzen bestaan over de interpretatie van de wet (zowel materieel als op het punt van bevoegdheid), kan het Comité een bindend besluit nemen. Hiervoor is een tweederde meerderheid vereist.

Vragen ?

paul.breitbarth@nymity.com | @EuroPaulB | +31.6.2493.6643

NYMITY
innovating compliance