Aanvulling op de aanzet tot een IT-Deltaplan voor de overheid: Langzaam & Snel

Theo Hooghiemstra (6 januari 2020)

In het publieke domein dient eerst de basis op orde te worden gebracht, voordat echt voortvarend aan zinvolle, veilige en betrouwbare innovatieve technologische toepassingen kan worden toegekomen, zoals effectieve inzet van AI en Blockchain.

De noodzakelijke basis die op orde dient te worden gebracht bestaat wat mij betreft met name uit een vertrouwensmodel van identificatie, authenticatie, autorisatie, logging en informatiebeveiliging overeenkomstig geldend Europees recht (eIDAS[1], Avg[2]) en onderliggende regels en standaarden, zoals de ISO 27001. Voor persoonlijke gezondheidsinformatie is deze ISO-norm in lijn met de Avg en gezondheidsrechtelijke wetgeving bijvoorbeeld vertaald in de NEN 7510: 2017 (informatiebeveiliging), in de NEN 7512 (vertrouwensbasis voor gegevensuitwisseling en 7513 (vereisten voor logging). Deze drie NEN-normen zijn in het Besluit Elektronische Gegevensverwerking Zorgaanbieders opgenomen dat onder de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg valt. Ik neem hier het voor mij vertrouwde veld van de gezondheidszorg als voorbeeld, maar dergelijke sector-specifieke uitwerkingen van eIDAS, Avg en bijvoorbeeld ISO-normen zijn er ook in de andere (publieke) sectoren.

Die noodzakelijke basis komt (te) traag op orde! Daar waar de maatschappelijke en technologische ontwikkelingen razend snel gaan, gaat de ontwikkeling van de daarvoor benodigde veilige en betrouwbare infrastructuur tergend langzaam.

Ik heb vooral ervaring in de gezondheidszorg en het zogenaamde identiteitsmanagement. In die werelden is te zien dat de basisvoorwaarden voor een veilige en betrouwbare (publieke) infrastructuur al zo'n 15 jaar (te) langzaam vooruit komt. De basis moet hier echt snel op orde komen! Alleen al vanwege eIDAS en Avg!

Bij het snel op orde brengen van een veilige en betrouwbare architectuur en infrastructuur kan en moet *Data Protection by Design of Default* de sleutel voor de oplossing zijn. Dat is niets nieuws en gaat eveneens erg traag. Het betreft namelijk de Avg-versie van het eerdere 'privacy by design' en privacy enhancing technologies (PET), waar oud AP/CBP-College-lid John Borking in 2010 op promoveerde en de Registratiekamer al in het jaar 1995 een Achtergrondstudie over publiceerde, waarvan in 2000 een gereviseerde versie verscheen.[3] Daar waar PET en 'privacy by design' vóór de Avg nog een aanbeveling was, is Data Protection by Design of

---

[1] EIDAS (Electronic IDentification Authentication and trust Services) is een Europese verordening "betreffende elektronische identificatie en vertrouwensdiensten

[2] De Algemene verordening gegevensbescherming is een Europese verordening (dus met rechtstreekse werking) die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.

[3] Privacy-enhancing technologies : the path to anonymity, Registratiekamer revised edition 2000 van de eerdere publicatie in 1995.

Default sinds de inwerkingtreding van de AVG een verplichting geworden! Het ontbreekt echter nog aan handhaving van deze verplichting sinds mei 2018.

Een groot deel van de Nederlandse wetgeving wordt uitgevoerd met behulp van ICT-systemen. Door de massaliteit waar de rijksoverheid, uitvoeringsorganisaties en decentrale overheden mee te maken hebben, is de inzet van ICT bij digitale uitvoering onmisbaar. Om de continue stroom nieuwe wetgeving goed en snel te kunnen implementeren is kennisgebaseerd werken noodzakelijk. Hiermee kan de wendbaarheid van hun ICT-systemen worden vergroot, zoals mooi en wijs is verwoord in het proefschrift van Mariette Lokin over 'Wendbaar Wetgeven, 'De wetgever als systeembeheerder'.[4]
Dat zal bijdragen aan een veilige, betrouwbare en gebruiksvriendelijke verwerking van persoonsgegevens, mits de relevante wet- en regelgeving beter wordt gehandhaafd, zowel door de Europese en landelijke toezichthouders als in de dagelijkse praktijk. Bijvoorbeeld via auditors.

Tot besluit is het in verlengde van de dataminimalisatie-gedachte - die ten grondslag ligt aan 'Data Protection by Design of Default' - van belang dat er sprake is van data soevereiniteit en – waar mogelijk – decentrale opslag van data bij de burger/client zelf. Dat is niet alleen een informatie-technologisch vraagstuk, maar zeker bij de overheden ook een bestuurskundig en juridisch vraagstuk. Informatie zal moeten worden georganiseerd rond burgers in plaats van overheidsorganisaties. Dit vergt slim en bestendig toedelen van bevoegdheden, zodat de burger eindelijk echt centraal komt te staan en te maken krijgt met een overheid die zich voor het geheel verantwoordelijk voelt en daarnaar handelt.[5]

Mijn strategisch-juridisch advies op hoofdlijnen aan bestuurders & CIO's van Rijk en decentrale overheden

Neem de Europese verordeningen eIDAS en Avg, en meer in het bijzonder het daarin verplichte 'Data Protection by Design of Default' als uitgangspunt. Inclusief bijbehorende - vaak sectorale – wetgeving en standaarden. Met andere woorden ga uit van 'data-soevereiniteit'. Verwerk daarbij niet meer persoonsgegevens dan noodzakelijk en zet de burger/client echt centraal. Laat daarbij IT-professionals, bestuurskundigen en juristen (en wellicht ook andere disciplines) multidisciplinair samen werken vanaf het allereerste ontwerp. Stimuleer handhaving van de betreffende verplichtingen. Zo lang de toezichthouders onvoldoende van zich laten horen, doe het dan zelf met behulp van bijvoorbeeld auditors.

Mr.dr. Theo Hooghiemstra is directeur en oprichter van Hooghiemstra & Partners, strategisch-juridisch adviesbureau op het raakvlak van technologie en recht. Hij is tevens bestuurder van stichting MedMij en gepromoveerd op informationele zelfbeschikking.

---

[4] https://research.vu.nl/ws/portalfiles/portal/69432703/complete+dissertation.pdf

[5] Zie de uitstekende, recente column 'De overheid, organisatie zonder brein? 'van mijn collega mr.dr. Marlies van Eck in IP, vakblad voor informatieprofessionals, 09/2019.