mitopics
Regelt IT al 20 jaar!

Privacy werkend krijgen in contractrelaties

NEVI CM-dag
16 maart 2017

mr. drs. Walter H. van Holst

mitopics

Regelt IT *al 20 jaar!*

Programma

- Inleiding
- Relatie met bewerkers/verwerkers
- PIAs
- Samenwerking met FG/DPO
- Vragen

mitopics
Regelt IT *al 20 jaar!*

Inleiding

- Algemene Verordening Gegevensverwerking (AVG) gaat in op 25 mei 2018
- Meldplicht datalekken kenden wij al
- AVG voegt daar nog compliance-eisen aan toe

mitopics
Regelt IT *al 20 jaar!*

Relatie verwerker (1/2)

- Concrete criteria voor bewerkersovereenkomst

- Register van verwerkingsactiviteiten:
  - Art. 30(1) Elke **verwerkingsverantwoordelijke** en, in voorkomend geval, de vertegenwoordiger van de verwerkingsverantwoordelijke houdt een **register** van de **verwerkingsactiviteiten** die onder hun **verantwoordelijkheid** plaatsvinden. Dat register bevat alle volgende gegevens: (…)

mitopics
Regelt IT *al 20 jaar!*

Bewerkersovereenkomst

- Doel: onafgebroken keten van gezagsverhoudingen tussen eerste verantwoordelijke en laatste bewerker

mitopics
Regelt IT *al 20 jaar!*

Criteria AVG (art. 28 lid 3)

a) Instructiebevoegdheid verantwoordelijke
b) Geheimhoudingsovereenkomsten personeel
c) Beveiligingsverantwoordelijkheid
d) Regeling over onderaanneming en doorzetten plichten naar onderaannemers
e) Ondersteunen verantwoordelijke bij invullen rechten van betrokkene
f) Ondersteunen verantwoordelijke bij invullen beveiligings- en continuïteitsverplichtingen
g) Exitregeling
h) Auditbepaling

mitopics
Regelt IT *al 20 jaar!*

Omgang met bewerkers/verwerkers in het kader van de meldplicht datalekken

- Gaat de bewerker u daadwerkelijk informeren over alle relevante incidenten?
- Gaat de bewerker eventueel zelf meldingen doen aan de Autoriteit Persoonsgegevens?
- Ontvangt u per incident alle informatie die u nodig heeft?
- Hoe gaat de bewerker u informeren over de incidenten?
- Wordt u tijdig geïnformeerd over de incidenten?
- Wordt u op de hoogte gehouden van eventuele nieuwe ontwikkelingen rond het incident, en van de maatregelen die de bewerker treft om aan zijn kant de gevolgen van het incident te beperken en herhaling te voorkomen?
- Kunt u vaststellen dat u daadwerkelijk op de hoogte wordt gesteld van alle relevante incidenten, en dat de verstrekte informatie klopt?

mitopics
Regelt IT *al 20 jaar!*

Relatie verwerker (2/2)

“Art. 30(2) De verwerker, en, in voorkomend geval, de vertegenwoordiger van de verwerker houdt een register van alle categorieën van verwerkingsactiviteiten die zij ten behoeve van een verwerkingsverantwoordelijke hebben verricht. Dit register bevat de volgende gegevens:”

Praktijkvoorbeeld (1)

- Zorginstelling
- Neemt kernapplicatie af van SaaS-provider
- Contract is al twaalf jaar oud

Gegevenseffectbeoordeling/PIA

- Wanneer?

Art. 35(1) Wanneer een soort verwerking, **in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico inhoudt** voor de rechten en vrijheden van natuurlijke personen voert de verwerkingsverantwoordelijke **vóór de verwerking** een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Eén beoordeling kan een reeks vergelijkbare verwerkingen bestrijken die vergelijkbare hoge risico's inhouden.

PIA (2)

Een gegevensbeschermingseffectbeoordeling als bedoeld in lid 1 is met name vereist in de volgende gevallen:

a) een systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen, die is gebaseerd op geautomatiseerde verwerking, waaronder profilering, en waarop besluiten worden gebaseerd waaraan voor de natuurlijke persoon rechtsgevolgen zijn verbonden of die de natuurlijke persoon op vergelijkbare wijze wezenlijk treffen;

b) grootschalige verwerking van bijzondere categorieën van persoonsgegevens als bedoeld in artikel 9, lid 1, of van gegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10; of

c) stelselmatige en grootschalige monitoring van openbaar toegankelijke ruimten.

PIA (3)

- Toezichthouders kunnen lijsten opstellen van situaties waarin PIA verplicht zijn

PIA (4)

De beoordeling bevat ten minste:

a) een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;

b) een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;

c) een beoordeling van de in lid 1 bedoelde risico's voor de rechten en vrijheden van betrokkenen; en

d) de beoogde maatregelen om de risico's aan te pakken, waaronder waarborgen, veiligheidsmaatregelen en mechanismen om de bescherming van persoonsgegevens te garanderen en om aan te tonen dat aan deze verordening is voldaan, met inachtneming van de rechten en gerechtvaardigde belangen van de betrokkenen en andere personen in kwestie.

PIA (5)

- Systematische verwerking van beoogde verwerkingen: welke gegevens, welke middelen -> IT-architectuur
- Verwerkingsdoelen, juridische waardering
- Beoogde maatregelen: vernieuwingstrajecten?

Omgang met FG/DPO

- Nieuwe functie, verplicht:
  - Publieke sector
  - Organisaties met grotere, complexere, meer riskante verwerkingen van persoonsgegevens
    - Zorginstellingen
    - Onderwijs

mitopics
Regelt IT *al 20 jaar!*

Vragen?

- Per e-mail: w.van.holst@mitopics.nl

Overige informatie

- Nieuwsbrief: nieuwsbrief@mitopics.nl
- Internet: www.mitopics.nl