Algemene Verordening Gegevensbescherming

mr. ing. Nico M. Keijser CDPO

Stichting RB Studiekring Rotterdam
Register Belastingadviseurs

13 maart 2018

CV

Studie:
- HTS Economische Bedrijfstechniek
- Nederlands Recht

Werk:
- Sinds 1989 werkzaam in automatisering in diverse functies
- Sinds 1999 zelfstandig gevestigd.

Kwalificaties:
- Certified Data Protection Officer CDPO
- Lid Nederlands Genootschap van Functionarissen voor de Gegevensbescherming (NGFG) (FG bij diverse bedrijven en zorginstellingen)
- Gediplomeerd Gerechtelijk Deskundige (JPAO Leiden)
- Ingeschreven in het Landelijk Register Gerechtelijke Deskundigen (LRGD)
- Lid van de Nederlandse Vereniging van Beëdigde Informaticadeskundigen (NVBI)
- Als ICT-deskundige verbonden aan de Stichting Geschillenoplossing Automatisering (SGOA)
- Als arbiter verbonden aan het Nederlands Arbitrage Instituut (NAI)

Nevenfuncties:
- Secretaris van het LRGD - Landelijk Register van Gerechtelijke Deskundigen
- Secretaris van de NVBI - Nederlandse Vereniging van Beëdigde Informaticadeskundigen
- Vice-President van het EEEI – European Expertise & Expert Institute (Parijs)
- Voorzitter van het NFFI - Nederlands Financieel Forensisch Instituut

Agenda

- Theorie
  - Algemeen en begrippen
  - Algemene bepalingen, beginselen
  - Verwerken persoonsgegevens
  - Rechten van betrokkene
  - Algemene verplichtingen
  - Functionaris Gegevensbescherming
  - Sancties
- Praktijk

- Algemene Verordening Gegevensbescherming of AVG
- General Data Protection Regulation of GDPR

- Verordening 2016/679 van het Europees Parlement en de Raad
- 27 april 2016
- In werking op 25 mei 2018

AVG

- 173 overwegingen
- 99 artikelen
- Opvolger van de Wet Bescherming Persoonsgegevens
- Wetsvoorstel Uitvoeringswet AVG (UAVG)

  Het wetsvoorstel strekt tot uitvoering van de verordening en beoogt daarnaast geen zelfstandige effecten. Het met de verordening beoogde effect is verdergaande harmonisatie van privacyregelgeving, bescherming van persoonsgegevens en bevordering van vrij verkeer van gegevens binnen de Unie.
- Inrichting AP, overgangsregels

Autoriteit Persoonsgegevens

- Toezichthouder
- Samenwerking met Autoriteit andere landen
- Artikel 29-Werkgroep
  - onafhankelijke advies -en overlegorgaan van Europese privacytoezichthouders.
- Publicaties via de Website AP

Algemene Bepalingen

- Toepassing op geheel of gedeeltelijk geautomatiseerde verwerking, of in bestand bestemd voor verwerking
  Materiële toepasbaarheid, art. 2
- Toepassing op vestiging in EU, betrokkene in de EU bevind, diensten op de EU gericht
  Territoriale toepasbaarheid, art. 3

Beginselen

Definities (art. 4)

- Betrokken
- Verwerking: bewerking van persoonsgegevens
  verzamelen, vastleggen ordenen, structureren, opslaan, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken, verspreiden, aligneren of combineren, afschermen, wissen of vernietigen.
- Verwerkingsverantwoordelijke
- Verwerker
- Ontvanger

Beginselen

Definities (art. 4)

- Persoonsgegevens: alle informatie van een geïdentificeerd of identificeerbaar natuurlijke persoon

Elk gegeven waaruit iemands identiteit blijkt/kan blijken

- Bijzondere persoonsgegevens (art. 9)

ras of etnische afkomst, politieke, religieus of levensbeschouwing, lidmaatschap vakbond, genetische biometrische, gezondheid, seksueel gedrag of gerichtheid

Verwerken

Persoonsgegevens: ja, mits

Bijzondere persoonsgegevens: nee, tenzij

Persoonsgegevens ja, mits

- Rechtmatig, behoorlijk en transparant
- Welbepaalde uitdrukkelijk en gerechtvaardigde doeleinden, niet onverenigbaar
- Toereikend en ter zake dienend, beperkt tot noodzakelijk (minimale gegevensverwerking)
- Juist en geactualiseerd
- Niet langer dan nodig
- Passende technische en organisatorische maatregelen
- **Verantwoordingsplicht! '*accountability*'**

(Art. 5)

Rechtmatigheid

- Toestemming, in vrijheid gegeven
- Noodzakelijk uitvoering overeenkomst
- Wettelijke verplichting verantwoordelijke
- Vitale belangen betrokkene
- Taak algemeen belang of openbaar gezag
- Gerechtvaardigde belangen verantwoordelijke

(Art. 6)

Bijzondere Persoonsgegevens nee, tenzij

- Toestemming, uitdrukkelijke toestemming
- Verplichtingen arbeidsrecht, sociale zekerheid
- Vitale belangen
- Door Stichting, passende waarborgen, leden
- Eerder geopenbaard door betrokkene
- Rechtsvordering / Gerechten
- Preventie, arbeidsgeneeskunde
- Algemeen belang
- Statistische doeleinden

(Art. 9)

Rechten van betrokkene

- Rectificatie
- Vergetelheid
- Beperking verwerking (dus ook niet wissen)
- Kennisgeving beperking aan ontvangers
- Overdraagbaarheid gegevens,structuur
- Bezwaar ivm specifieke situatie, voorbijgaan
- Geen geautomatiseerde besluiten, profilering

(Art. 16-22)

Algemene Verplichtingen

- Passende technische & organisatorische maatregelen
- Gegevensbeschermingsbeleid organisatie
- Privacy by design, privacy by default
- Verwerkers met afdoende garanties
- Register van verwerkingsactiviteiten
- Incidentenregister
- Verantwoordingsplicht

(Art. 24 e.v.)

Functionaris Gegevensbescherming

Verwerkingsverantwoordelijke en de Verwerker wijzen een FG aan:

- Overheidsinstantie (Gerechten niet voor gerechtelijke taken)
- Stelselmatige en regelmatige observatie
- Verwerking hoofdzakelijk grootschalige bijzondere persoonsgegevens (9) en strafbare feiten (10)
- Alle overige gevallen niet verplicht

(Art. 37)

Positie van de FG

- Naar behoren en tijdig betrokken
- Toegang tot alle gegevens, en activiteiten
- Benodigde middelen verschaffen
- Geen instructies van verantwoordelijke
- Betrokkenen kunnen contact opnemen
- Geheimhouding
- Aanmelden bij de AP
- Ontslagbescherming conform OR

Taken van de FG

- Informeren en adviseren over AVG
- Toezien op de naleving AVG en beleid
- Desgevraagd advies verstrekken over PIA
- Met de AP samenwerken
- Optreden als contactpunt voor AP

Sancties (1)

Doeltreffend, evenredig en afschrikkend
- Aard, ernst en duur,
- Opzet of nalatigheid
- Mate van verantwoordelijkheid
- Maatregelen beperking schade
- Technische & Organisatorische maatregelen
- Eerdere relevante inbreuken
- Mate samenwerking AP
- Categorieën persoonsgegevens gelekt
- Kennisname door AP, wie heeft gemeld
- Elke andere omstandigheid rondom het geval

Sancties (2)

- € 10.000.000,00 of 2% van de jaarlijkse omzet
  Inbreuken op artt. 8, 11, 25-39, 42 en 43
- € 20.000.000,00 of 4% van de jaarlijkse omzet
  Basisbeginselen inzake verwerking, artt. 5, 6, 7 en 9, rechten betrokkenen artt. 12-22

(Art. 83)

Sancties (3)

Naast of in plaats van maatregelen
Art. 58 lid 2 a)-h) en j)

Waarschuwingen, berisping, gelasten uitvoering, gelasten werkwijze, melden inbreuk, verwerking beperken of verbieden, rectificatie te gelasten, certificering intrekken, doorgifte opschorten

Praktijk

- Verwerkingenregister
- Verwerkingen
- Incidentenregister
- Verwerkersovereenkomst
- Persoonsgegevens bij Belastingadviseur
- Technische en Organisatorische maatregelen
- Privacyreglement
- Rechten van betrokkenen
- Verwerkers
- Gedragscode
- Incidenten en datalekken
- Bewustwording

Doel en Middelen

Wie Verwerkingsverantwoordelijke en Verwerker is bepaalt de feitelijke situatie.
Je kunt die hoedanigheid niet “contracteren”.

Niet omdraaien: Omdat ik Verwerkingsverantwoordelijke ben mag ik doel en middelen vaststellen

Rol Adviseurs

- Verwerkingsverantwoordelijke – Verwerker
- Gezamenlijke Verwerkingsverantwoordelijke

- Eenmalige ontvangst van persoonsgegevens, daarna zelfstandige rol
- Informeren van betrokkenen volgens Art. 14 AVG

Verwerkingenregister

Elke Verwerkingsverantwoordelijke houdt een register

- Naam, contactgegevens, gedeelde verantwoordelijke, FG
- Verwerkingsdoeleinden
- Beschrijving categorieën betrokkenen
- Beschrijving categorieën persoonsgegevens
- Ontvangers en Doorgiften
- Bewaartermijnen
- Technische & Organisatorische maatregelen

(Art.30)

Art 30 lid 5

5. De in de leden 1 en 2 bedoelde verplichtingen zijn niet van toepassing op ondernemingen of organisaties die minder dan 250 personen in dienst hebben,
Tenzij
het waarschijnlijk is dat de verwerking die zij verrichten een risico inhoudt voor de rechten en vrijheden van de betrokkenen,
de verwerking niet incidenteel is,
of de verwerking bijzondere categorieën van gegevens, als bedoeld in artikel 9, lid 1,
of persoonsgegevens in verband met strafrechtelijke veroordelingen en strafbare feiten als bedoeld in artikel 10
betreft.

De uitzonderingen zijn dus minimaal.

Verwerkingen

Wat zijn “verwerkingen”?

- Backoffice / Dossier applicatie
- Mailprogramma
- Tekstverwerkings- , Spreadsheet bestanden
- Losse bestanden (bijv. scans)
- Eigen salarisadministratie
- Alle bestanden voor cliënten

Incidentenregister

Melden binnen 72 uur
- Aard van de inbreuk
- Categorieën van betrokkenen
- Categorieën van persoonsgegevens
- Aantal betrokkenen
- Genomen maatregelen inbreuk
- Genomen maatregelen gevolgen te mitigeren

(Art. 33) Zie ook website AP, “melden”

Verwerkersovereenkomst

- Uitsluitend verwerken op basis van instructie
- Vertrouwelijkheid werknemers
- Beveiliging
- Geen subverwerkers inhuren zonder toestemming
- Passende T&O Maatregelen
- Informatie verstrekken ivm incidenten (register)
- Wissen of retourneren
- Informatie en Audits
- Verwerkingenregister bijhouden

(Art. 28 AVG)

Verwerkersovereenkomst

- Niet in Algemene Voorwaarden regelen
- De verwerking door een verwerker wordt geregeld in een overeenkomst …
- Onverminderd een individuele overeenkomst tussen Verwerkingsverantwoordelijke en de Verwerker …..

(Art. 28 lid 3 en lid 6 AVG)

Belastingadviseurs

- Verwerken Persoonsgegevens
  - NAW, geboortedata, bankrekeningen, verzekeringsgegevens, salarisgegevens, …..
- Verwerken Bijzondere Persoonsgegevens
  - pasfoto's, gegevens over gezondheid, medische behandelingen, allergieën, lidmaatschappen vakbonden, kerkgenootschappen, …..

Beveiliging

Rekening houdend met

- de stand van de techniek
- uitvoeringskosten
- aard, omvang context en doeleinden
- waarschijnlijkheid en ernst van risico

treft de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen

Passende T&O maatregelen

- Kantooromgeving

  alarminstallatie, kasten met slot, clean desk, clear screen, bewustzijn medewerkers, melden incidenten en vermeende datalekken
- Automatisering

  toegangsbeveiliging (fysiek en digitaal), inzage op basis van functie, SaaS, 2FA, veilige encrypted back-up, virusbeveiliging, firewalls, *intrusion detection*

Toegang tot omgeving

- Werken “van huis uit”
  - Beperken van toegang op basis van IP adres
  - 2 factor authenticatie
- Gegevens op mobiele apparatuur
  - Wachtwoord, toegangscode
  - 2 factor authenticatie
- E-mail op mobiele apparatuur
  - Toezending bestanden
  - Via een beveiligd portal
- Toegang cliënt tot eigen dossier

Privacyreglement (1)

Privacyreglement (2)

Artikel 1.
Wij werken volgens de geldende regelgeving op het gebied van Gegevensbescherming

Artikel 2.

Inwerkingtreding

Rechten van betrokkenen (1)

Kan dit binnen uw organisatie en software?

- Rectificatie
  - inherent aan werk
- Vergetelheid
  - Toestemming ingetrokken
  - Let op eigen bewaarplichten
- Beperking verwerking
  - Tijdelijk niet verwerken, voor controle van (andere) gegevens
- Kennisgevingsplicht beperking
  - Doorgeven aan ontvangers, tenzij onmogelijk of onevenredige inspanning

Rechten van betrokkenen (2)

- Overdraagbaarheid gegevens
  - dossier overdragen
  - duidelijke structuur
- Bezwaar
  - Verwerking staken tenzij dwingende gerechtvaardigde gronden
- Geen geautomatiseerde besluiten, profilering
  - Tenzij toestemming
  - Niet voor bijzondere persoonsgegevens

Verwerker

- Maakt u gebruik van verwerkers?
  - Dienstverleners - ZZP-ers
- Software van derden?
- Software as a Service (SaaS) provider?
- Wie pleegt onderhoud?
- Wie heeft toegang?
- Waar en hoe wordt back-up uitgevoerd?

Verwerkersovereenkomst sluiten

Gedragscode

- Werken volgens een goedgekeurde gedragscode is element om aan te tonen dat de verplichtingen worden nagekomen
- Gedragscode van beroepsorganisatie
- Goedgekeurd door de Autoriteit Persoonsgegevens

Incidenten

- Houdt een register bij
- Documenteer ieder incident: “inbreuk op de beveiliging”
- Intern en extern
- Onderzoek het incident
- Is het een datalek?

Wat zijn incidenten?

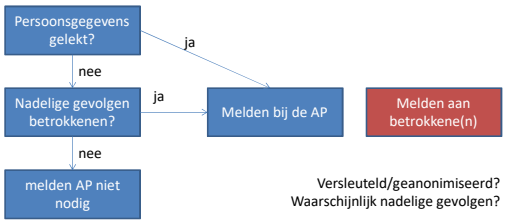
- Post verkeerd verzonden, geopend retour
- Aan-, CC-, BCC- fout bij mail verzenden
- Gegevens verwijderd, Back-up terugzetten noodzakelijk
- Ransomware, Malware, Virussen, Hackaanval
- Inbraak in kantoor
- Diefstal, verliezen computer, mobile, tablet
- Personeel uit dienst met toegang en wachtwoord
- Foute toegangsstructuur in programma

Zijn het ook datalekken?

- Post verkeerd verzonden, geopend retour
- Aan-, CC-, BCC- fout bij mail verzenden
- Gegevens verwijderd, Back-up terugzetten noodzakelijk
- Ransomware, Malware, Virussen, Hackaanval
- Inbraak in kantoor
- Diefstal, verliezen computer, mobile, tablet
- Personeel uit dienst met toegang en wachtwoord
- Foute toegangsstructuur in programma

Datalekken

- Wet meldplicht datalekken
- Onderzoek: Is het incident ook een datalek?



Versleuteld/geanonimiseerd?
Waarschijnlijk nadelige gevolgen?

Bewustwording

- Algemene informatie verstrekken (AP)
- Specifieke informatie verstrekken (Branche)
- Open klimaat creëren over vragen en incidenten,
- Privacyreglement
- Stimuleren het goed te doen
- Meldingsformulier of procedure maken
- Mensen erkennen, deel van de oplossing maken

Informatie AP

- Informatie
  - Onderwerpen als:
    Beveiliging, Financiën, Identificatie, Werk en uitkering
- 10 stappen AP
  - http://keijserconsultancy.nl/ap-10stappen/
  - https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/in_10_stappen_voorbereid_op_de_avg.pdf
- Melden
  - datalekken
- Nieuwsbrief

www.autoriteitpersoonsgegevens.nl

Vragen?

Nico Keijser
info@keijserconsultancy.nl
06-51149629