UITVOERINGSORGANISATIE BEDRIJFSVOERING RIJK

Uitvoeringsorganisatie
Bedrijfsvoering Rijk
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Bijeenkomst PUC **update informatiebeveiliging**

Rian van Delft
coördinator informatiebeveiliging

K-O-O-P
Kennis- en Exploitatiecentrum Officiële Overheidspublicaties

Den Haag | 21 maart 2018

Het onderwerpen van vandaag

- Informatiebeveiliging bij KOOP
  - BIR
  - ICV
  - DigiD
  - AVG en PUC

K-O-O-P

Kennis- en Exploitatiecentrum
Officiële Overheidspublicaties

Baseline Informatiebeveiliging Rijksdienst (BIR)

- Versie 2012
  tactisch normenkader (TNK)
- ISO 27000
- Versie 2017
  (BIR 2.0)
- Toekomst: BIO?

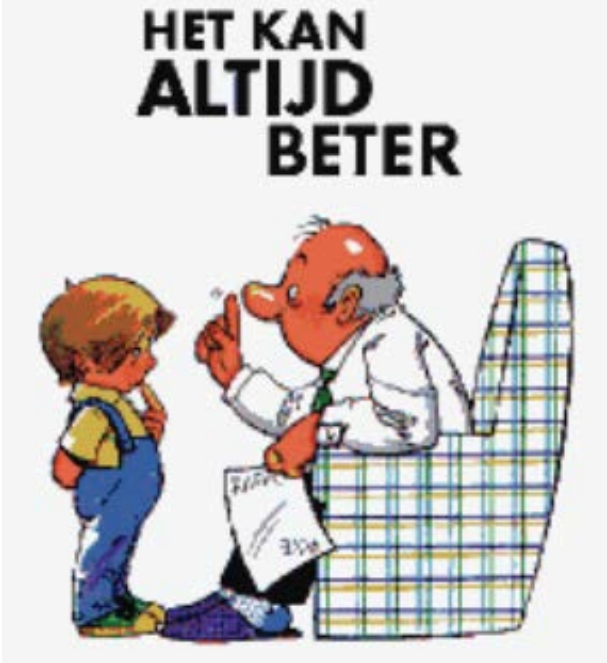
Interne controle op BIR

Beveiligingsdoctabel blad	Nummer	R/R	Omschrijving in BIR	Opmerking	van Rick (2013)	van Rian (2014/2015/2016) met docs	check 1	check 2	check 3	check 4	check 5	44 = aantal = gedaan
							2017 R	2017 R	2017	2017	2017	2017
		(35 stuks)			Toelichting (vrije tekst) in rood: toevoegingen in 2017	aantoonbaar dmv de volgende documenten (zie tabel met verwijzingen) toevoegingen 2015 en 2016 in blauw in rood: toevoegingen: 2017 in groen: geen doc of dir	2015 Solv-check: selectie op: R + Solv(AA)	2015 Solv-check: selectie op: R + niet-Solv(AA) = dus overig R	2015 Solv-check: selectie op: X bij Systeem R - ASP(AA)	2015 Solv-check: selectie op: ASP(AA) R - (geldt ook voor niet-Solv-dienstverlen	2015 rest / overige R- ASP-	som vorige kolommen tbv selectie leeg = wit vol = blauw
11.4.5			Scheiding van netwerken: Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.									
	11.4.5.1	R	Werkstations worden zo ingericht dat routeren van verkeer tussen verschillende zones of netwerken niet mogelijk is.		Geimplementeerd door service provider	Verwezen wordt naar de service providers: hosting (ASP4all), ICT-werkplek (BZK resp SSC-ICT). Informatiebeveiligingseisen voor leveranciers (v1.0) Uitgangspunten IT infrastructuur	o.a. VPN tussen KOOP en Solvinty OTAP					o.a. VPN tussen KOOP en Solvinty OTAP
	11.4.5.2	R	De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal een keer per jaar, geevalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.	De A geldt voor de eigenaar van het netwerk	KOOP heeft een document opgesteld met uitgangspunten voor zonering en andere inrichtingskeuzes (Uitgangspunten IT infrastructuur), dat is gebaseerd op architectuurprincipes die KOOP hanteert. ASP4All beschikt over overzichten welke systemen in welke zone staan.	Uitgangspunten IT infrastructuur Technische Ontwerpen		KOOP aangelegenheid OTAP				KOOP aangelegenheid OTAP
	11.4.5.3	R	Elke zone heeft een gedefinieerd beveiligingsniveau Zodat de filtering tussen zones is afgestemd op de doelstelling van de zones en het te overbruggen verschil in beveiligingsniveau. Hierbij vindt controle plaats op protocol, inhoud en richting van de communicatie.		Geimplementeerd door service provider	Verwezen wordt naar de service providers: hosting (ASP4all), ICT-werkplek (BZK resp SSC-ICT). Informatiebeveiligingseisen voor leveranciers (v1.0) Uitgangspunten IT infrastructuur Technische Ontwerpen	er is compartimentering horizontaal en verticaal zie TO's Incl OTAP scheiding					er is compartimentering horizontaal en verticaal zie TO's Incl OTAP scheiding
	11.4.5.4	R	Beheer en audit van zones vindt plaats vanuit een minimaal logisch gescheiden, separate zone.		Geimplementeerd door service provider	Verwezen wordt naar de service providers: hosting (ASP4all), ICT-werkplek (BZK resp SSC-ICT). Informatiebeveiligingseisen voor leveranciers (v1.0) Uitgangspunten IT infrastructuur Technische Ontwerpen Pentestrapporten	becop is separate applicatie met separate inlog					becop is separate applicatie met separate inlog
					Geimplementeerd door service provider	Uitgangspunten IT infrastructuur						

11.4.5.2	R	De indeling van zones binnen de technische infrastructuur vindt plaats volgens een operationeel beleidsdocument waarin is vastgelegd welke uitgangspunten voor zonering worden gehanteerd. Van systemen wordt bijgehouden in welke zone ze staan. Er wordt periodiek, minimaal een keer per jaar, geevalueerd of het systeem nog steeds in de optimale zone zit of verplaatst moet worden.

PUC en BIR

- In 2017 focus op accountbeheer
- Actiepunten gereed (?)



In Control Verklaring (ICV)

- Jaarlijks bij KOOP op OEB
- Vanwege Risicokaart MinBZK
  te beschermen belangen
- Selectie op BIR:2012
  95 doelstellingen/maatregelen
  explains
- CIO BZK

DigiD Assessment

- Als je DigiD gebruikt
  → jaarlijks assessment + pentesten
- DigiD-OP
- 9 pentesten, o.a. PUC Open Data
- Gebaseerd op NCSC-richtlijnen voor webapplicaties

Algemene Verordening Gegevensbescherming (AVG)

- AVG = GDPR

- Vervangt Wet Bescherming Persoonsgegevens (Wbp)
  .. na publicatie Uitvoeringswet [uAVG] ..

- In werking sinds 24 mei 2016
- Van toepassing vanaf 25 mei 2018

AUTORITEIT PERSOONSGEGEVENS

Persoonsgegeven

- Ieder gegeven

  … betreffende

  … een geïdentificeerde of identificeerbare

  … natuurlijke persoon

  … = de betrokkene

Betekenis AVG

- Beschrijving welke persoonsgegevens over betrokkenen noodzakelijk
- Hoe daarmee omgegaan wordt
- Hoe rechten van betrokkenen worden gewaarborgd (privacy)

In PUC

- Persoonsgegevens in, of tbv accounts
- Persoonsgegevens vaak niet in de content
- Persoonsgegevens vaak niet in de metagegevens

Hoe inspelen op AVG?

- Maken Privacy Impact Assessment (PIA)
  - = Gegevensbeschermings Effect Beoordeling (GEB)
  - Model PIA 2.0/2017

Model gegevensbeschermings-effectbeoordeling rijksdienst (PIA)

De GEB = PIA

- 17 onderdelen; in **4 delen**: ABCD (+E)
- Verplicht advies door de functionaris gegevensbescherming
- PIA/GEB = continu proces, ook na deadline

- Bij BZK coördinatie via centrale projectleider invoering AVG (CIO-office)
- Bij KOOP: >20 PIA's

A. Beschrijving algemene kenmerken gegevensverwerkingen (1)

1. Voorstel
   → Welk object/applicatie?
   PUC -> generiek vs specifiek
2. Persoonsgegevens
   → Wat leg je vast?
   accounts: naam, organisatie, email-adres
3. Verwerkingen
   → Hoe worden de gegevens verwerkt?
   registratie, verzending, (niet)openbaar
4. Doelen
   → Waarom doe je dit?
   authenticatie en autorisatie; ...

A. Beschrijving algemene kenmerken gegevensverwerkingen (2)

5. Betrokken partijen
   → Welke organisaties/rollen/personen?
   opdrachtgever, KOOP, hostingprovider, …

Onderscheid maken tussen

A. degene die input levert

B. degene die verwerkt (verwerker)

C. opdrachtgever (verwerkingsverantwoordelijke)

D. gebruiker/raadpleger

E. betrokkene (over wie info wordt vastgelegd)

NB (verwerkers)overeenkomsten

Rollen

Verwerkings-verantwoordelijke

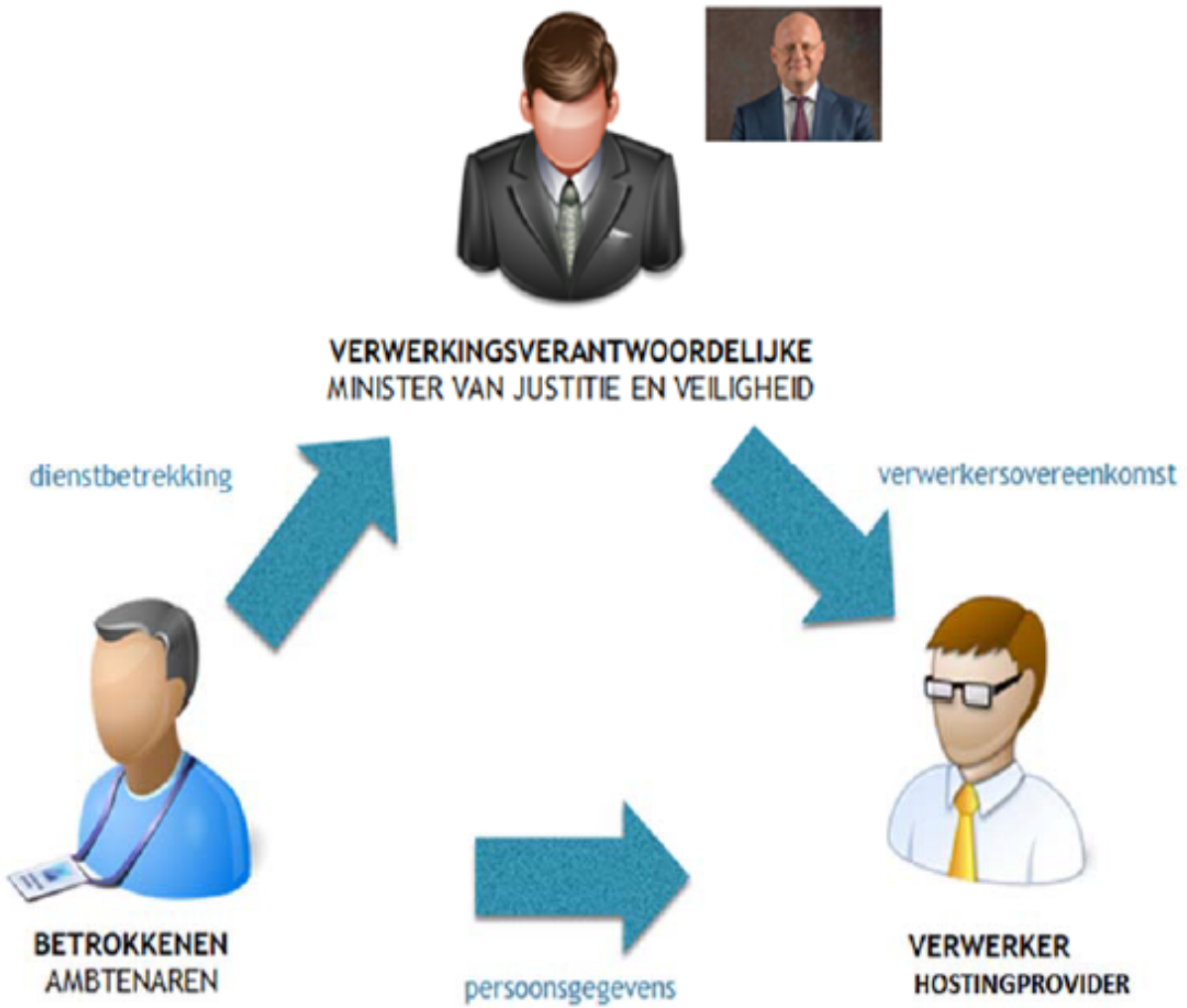
- stelt het doel van en de middelen voor de verwerking vast

Verwerker

- verwerkt gegevens ten behoeve van de verantwoordelijke

Betrokkene

- degene op wie een gegeven betrekking heeft



A. Beschrijving algemene kenmerken gegevensverwerkingen (2)

5. Betrokken partijen
   → Welke organisaties/rollen/personen?
   opdrachtgever, KOOP, hostingprovider, …
6. Belangen bij de verwerking
   → Wie doet wat waarom?
   publicatie/raadpleegbaarheid
7. Verwerkingslocaties
   → Waar?
   bij hostingprovider via KOOP; NL; of anders
8. Techniek
   → Automatische besluitvorming? Profiling?
   niet, evt. Piwik (gebruiksstatistieken)

A. Beschrijving algemene kenmerken gegevensverwerkingen (3)

9. Juridisch en beleidsmatig kader
   → Welke (overige) wet en regelgeving?
   - Beleidskaders Informatievoorziening Rijk (o.a. VIR, BIR:2012/2017, ...)

10. Bewaartermijnen
   → Hoelang bewaren, archivering?
   - permanent? (selectielijst)
   - account actief vs geblokkeerd vs verwijderd

B. Beoordeling rechtmatigheid gegevensverwerkingen (1)

11. Grondslag

→ Achtergrond, bron van het waarom?

… regelgeving omtrent de content

Grondslagen verwerking

- Functionaris Gegevensbescherming (13 feb 2018) over accounts en toestemming:
  De betrokken bevoegde ambtenaar heeft geen keus. Hij moet wel de gegevens opgeven. Toestemming werkt niet in gezagsrelaties.

B. Beoordeling rechtmatigheid gegevensverwerkingen (1)

11. Grondslag
    → Achtergrond, bron van het waarom?
    … regelgeving omtrent de content
12. Bijzondere en strafrechtelijke persoonsgegevens
    → Gevoeligheid?
    niet gevoelig (bijv. geen BSN)
13. Doelbinding
    → Uitsluitend voor gebruik oorspronkelijk doel?
    ja; andere doelen zijn niet toegestaan

B. Beoordeling rechtmatigheid gegevensverwerkingen (2)

14. Noodzaak en evenredigheid

→ Proportionaliteit?

(doel gerechtvaardigd tov inbreuk privacy?)

ja, deze info is noodzakelijk

→ Subsidiariteit?

(kan het niet anders?)

nee, het moet wel digitaal

B. Beoordeling rechtmatigheid gegevensverwerkingen (3)

15. Rechten van betrokkene

→ recht op inzage & correctie

accounts: contact servicedesk KOOP,
mits akkoord opdrachtgever; ook: account-check

overig: via (onze) opdrachtgever

→ recht op verwijdering ('vergetelheid')

contact servicedesk KOOP;
(onze) opdrachtgever bepaalt

C. Beschrijving en beoordeling risico's voor de rechten en vrijheden betrokkene

16. Risico's

→ Zijn er mogelijk negatieve gevolgen?
→ Oorsprong van die gevolgen?
→ Waarschijnlijkheid van optreden gevolgen?
→ Ernst/impact van gevolgen?

D. Beschrijving (voor)genomen maatregelen

17. Maatregelen

→ Technisch?
→ Organisatorisch?
→ Juridisch?

→ (acceptabele) Restrisico's?

Halen we 25 mei 2018?

- Policy:
  - In Control per 25 mei 2018 (PIA OK + actiepunten [E])

  en
  - Compliant per 31 december 2018 (actiepunten gereed)

Samengevat

- BIR, ICV, DigiD, AVG/PIA, PUC
- Stapsgewijs uitbreiden

Zijn er nog vragen ?!