INFORMATIE BEVEILIGINGS DIENST

Privacy voor de CISO

John van Huijgevoort (IBD) & gemeentelijke CISO / FG

15-02-2022

1

INFORMATIE BEVEILIGINGS DIENST

Agenda

- Algemene verordening gegevensbescherming (AVG)
- Privacyfunctionaris
  - Functionaris voor de Gegevensbescherming (FG)
  - Privacy Officer (PO)
- Data Protection Impact Assessment (DPIA)
  - Integrale Risico en Privacy Analyse (IRPA)
- Datalekken
- AVG Borgingsproduct 2.0
- FG Rapportages
- Samenwerking
- Discussiepunten!

2

INFORMATIE BEVEILIGINGS DIENST

Algemene verordening gegevensbescherming (AVG)

- Vanaf 25 mei 2018 in alle landen van de Europese Unie (EU) geldt.
  - plus Liechtenstein, IJsland en Noorwegen
    - Europese Economische Ruimte (EER)
  - Persoonsgegevens mogen ook verstuurd worden naar derde landen, **met een passend beschermingsniveau**.
    - Bijvoorbeeld Adequaatheidsbesluit of Standard Contractual Clauses (SCC) / Modelcontracten.
  - General Data Protection Regulation (GDPR)
- Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)

INFORMATIE BEVEILIGINGS DIENST

Autoriteit Persoonsgegevens (AP)

- Nederlandse toezichthouder
  - Doet onderzoek (bijvoorbeeld na klachten)
  - Bij overtreding handhavend optreden (boetes opleggen)
  - Mogelijkheid voorafgaande raadpleging (bij hoge privacyrisico's)
- Publiceert richtlijnen die onderwerpen uit de AVG verduidelijken

INFORMATIE BEVEILIGINGS DIENST

AVG Highlights

- Stel **Functionarissen voor gegevensbescherming (FG)** aan.
- Hou controle op de verwerkingen.
  - Hou overzicht van de verwerkingen bij en up-to-date (**Verwerkingsregister**).
  - Bepaal **grondslag** verwerking.
  - Bepaal of **Data Protection Impact Assessment (DPIA)** noodzakelijk is.
  - Sluit **verwerkingsovereenkomsten** met (verwerkers).
- Pas '**privacy by design**' en '**privacy by default**' toe.
- Stel procedure **meldplicht datalekken** op.
- Zorg dat mensen hun **privacyrechten** kunnen uitoefenen.

5

INFORMATIE BEVEILIGINGS DIENST

Grondslagen

Zes grondslagen voor het verwerken van persoonsgegevens:

1. Toestemming
2. Overeenkomst
3. Wettelijk verplicht
4. Vitale belangen
5. Algemeen belang of openbaar gezag
6. Gerechtvaardigde belang

6

INFORMATIE BEVEILIGINGS DIENST

AVG rollen

- (gezamenlijke of zelfstandig) **verwerkingsverantwoordelijke** (meestal opdrachtgever).
- **Verwerker** (meestal opdrachtnemer).

7

INFORMATIE BEVEILIGINGS DIENST

Rechten van betrokkenen

Het recht:

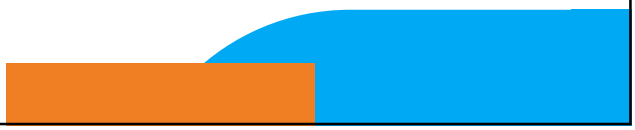
- op inzage
- op gegevenswissing (vergetelheid)
- op rectificatie
- op overdraagbaarheid (dataportabiliteit)
- op beperking van de verwerking
- op informatie
- van bezwaar
- niet te worden onderworpen aan geautomatiseerde individuele besluitvorming / profilering

8

INFORMATIE BEVEILIGINGS DIENST

Functionaris voor de Gegevensbescherming (FG)

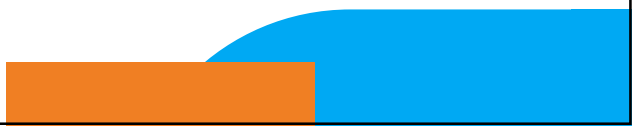
- Aanstelling FG is **verplicht**
- Door **bestuursorganen gemeenten** en samenwerkingsverbanden
  - Advies: gezamenlijk één FG aanstellen
  - De verwerkingsverantwoordelijke en de verwerker blijven verantwoordelijk voor de naleving van de verplichtingen op grond van de AVG, **niet** de FG
  - Ook kunnen verschillende (regio)gemeenten kiezen om gezamenlijk één FG aan te stellen.
- Plichten van de verwerkingsverantwoordelijke
  1. Waarborgen autonomie en onafhankelijkheid van de FG
  2. Betrekken van de FG bij privacy aangelegenheden
  3. Ondersteuning bieden en middelen verschaffen aan de FG



INFORMATIE BEVEILIGINGS DIENST

Waarborgen autonomie en onafhankelijkheid FG

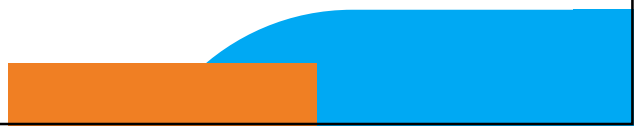
- Geen instructies.
- Geen belangenconflict.
- Positionering binnen gemeentelijke organisatie.
  - Positie die autonomie en onafhankelijkheid van de FG waarborgt (staffunctie).
- Ontslagbescherming.
- Verankering in beleid.



INFORMATIE BEVEILIGINGS DIENST

Betrek FG bij alle privacyaangelegenheden

- Cruciaal dat de FG **zo vroeg mogelijk betrokken wordt** bij alle aangelegenheden die de bescherming van persoonsgegevens raken.
- **Geraadpleegd** worden bij datalekken en beslissingen met gevolgen voor gegevensbescherming.
- **Geraadpleegd** worden bij DPIA.



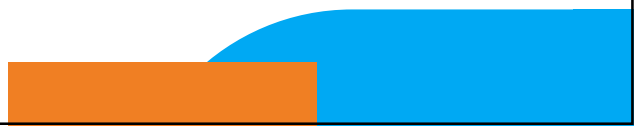
11

INFORMATIE BEVEILIGINGS DIENST

Stel middelen beschikbaar aan FG

Een gemeentelijke verwerkingsverantwoordelijke moet de FG ten minste de volgende middelen bieden:

- Tijd.
- Ondersteuning.
- Financiële middelen, infrastructuur & personeel.
- Toegang.
- Opleidingsbudget.
- Bescherming.



12

INFORMATIE BEVEILIGINGS DIENST

Taken FG

1. Adviseren
2. Toezien op naleving
3. Samenwerking met en contactpunt van de AP
4. Optreden als contactpunt voor betrokkenen

- Bij de uitvoering van zijn taken **een risico gebaseerde aanpak hanteren**.
  - Activiteiten prioriteren en werkzaamheden richten op verwerkingen met een hoog risico.

INFORMATIE BEVEILIGINGS DIENST

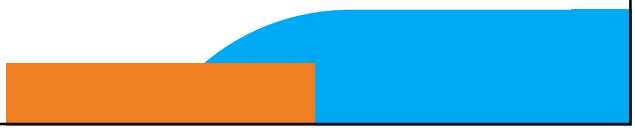
Taken FG – Adviseren

- Legt verslag af over de stand van zaken is ten aanzien van privacy compliance bij de gemeente
- Verwerkingsverantwoordelijke moet bij de uitvoering van een DPIA advies vragen van de FG
- Adviseren over techniek en beveiliging (sparren met bijvoorbeeld de CISO of security adviseur)
- Adviseren naar aanleiding van audits
- Datalekken

INFORMATIE BEVEILIGINGS DIENST

Taken FG –Toezien op naleving

- Toezien dat binnen de gemeente de AVG wordt nageleefd.
  - Beschikt niet over sanctiebevoegdheden.
- Bevoegdheden
  - Inzage en (klachten)onderzoek
  - Vragen van inlichtingen
  - Betreden van ruimten

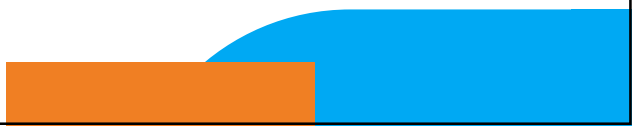


15

INFORMATIE BEVEILIGINGS DIENST

Privacy Officer (PO)

- Richt zich op de daadwerkelijke implementatie
  - Verantwoordelijk voor het ontwikkelen en bewaken van het privacybeleid en het ondersteunen van de uitvoering
- Dagelijkse aanspreekpunt voor medewerkers wat betreft gegevensbescherming.
- Geen toezichthoudende bevoegdheden
- Combineren rol PO en FG niet wenselijk
  - De CISO en PO rollen passen beter bij elkaar!



16

INFORMATIE BEVEILIGINGS DIENST

Kennis en vaardigheden FG

De FG wordt aangewezen op grond van zijn professionele kwaliteiten en zijn vermogen om zijn taken te vervullen.

- Brede en toereikende kennis.
- Het vermogen om binnen de organisatie een cultuur van gegevensbescherming te bevorderen.
- Soft skills en gevoel voor politiek-bestuurlijke verhoudingen.

Kennis van wetgeving en ICT gecombineerd in één persoon is schaars.

- Er zal naar een praktische oplossing dienen te worden gezocht, waarbij de FG niet noodzakelijkerwijs een jurist hoeft te zijn.

17

INFORMATIE BEVEILIGINGS DIENST

DPIA

Wat

- Een DPIA is een instrument om **vooraf de privacyrisico's** van een gegevensverwerking in kaart te brengen. En om **daarna maatregelen te kunnen nemen** om de risico's te verkleinen.
- Ook wel gegevensbeschermingseffectbeoordeling.

Wie

- **De verwerkingsverantwoordelijke zorgt ervoor dat de DPIA wordt uitgevoerd**. De verwerkingsverantwoordelijke kan de DPIA door iemand anders laten uitvoeren, maar de verwerkingsverantwoordelijke blijft eindverantwoordelijk.
  - De PO kan hierbij ondersteuning verlenen.

18

INFORMATIE BEVEILIGINGS DIENST

Waarom een DPIA?

Verplichting
- Sprake van hoog privacyrisico voor betrokkenen
- Lijst van AP
- Criteria van de Europese privacytoezichthouders (EDPB)

DPIA uitvoeren voor een bestaande verwerking?
- Ja, soms moet alsnog een DPIA worden uitegvoerd voor een bestaande verwerking.
  - Bij verandering aan het risico van de gegevensverwerking en (na de verandering) een hoog privacyrisico oplevert.

Geen DPIA nodig
- Niet nodig een DPIA uit te voeren als:
  - De gegevensverwerking géén hoog privacyrisico oplevert;
  - Er is een voorafgaand onderzoek door de AP uitgevoerd en de verwerking is in de tussentijd niet veranderd;
  - De risico's van de verwerking zijn niet veranderd.

19

INFORMATIE BEVEILIGINGS DIENST

AVG - DPIA verplicht

- Systematisch en uitgebreid persoonlijke aspecten evalueert **gebaseerd op geautomatiseerde verwerking**, waaronder profiling, en waarop besluiten worden gebaseerd die gevolgen hebben voor mensen.
- Op grote schaal **bijzondere persoonsgegevens of strafrechtelijke gegevens** worden verwerkt.
- Op **grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied**.

20

INFORMATIE BEVEILIGINGS DIENST

AP-lijst - DPIA verplicht

1. Heimelijk onderzoek
2. Zwarte lijsten
3. Fraudebestrijding
4. Creditscores
5. Financiële situatie
6. Genetische persoonsgegevens
7. Gezondheidsgegevens
8. Samenwerkingsverbanden
9. Cameratoezicht
10. Flexibel cameratoezicht
11. Controle werknemers
12. Locatiegegevens
13. Communicatiegegevens
14. Internet of things
15. Profilering
16. Observatie en beïnvloeding van gedrag
17. Biometrische gegevens

INFORMATIE BEVEILIGINGS DIENST

Criteria EDPB - DPIA aanbevolen

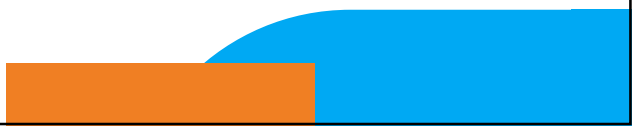
- Beoordelen van mensen op basis van persoonskenmerken
- Geautomatiseerde beslissingen
- Stelselmatige en grootschalige monitoring
- Gevoelige gegevens
- Grootschalige gegevensverwerkingen
- Gekoppelde databases
- Gegevens over kwetsbare personen
- Gebruik van nieuwe technologieën
- Blokkering van een recht, dienst of contract

Als vuistregel kunt u hanteren dat u een DPIA moet uitvoeren als uw verwerking aan 2 of meer van de bovenstaande 9 criteria voldoet.

INFORMATIE BEVEILIGINGS DIENST

Integrale Risico en Privacy Analyse Privacy

- De Ethische Data Assistent (DEDA)
  - Moet ik dit eigenlijk wel willen?
- Pre-DPIA
  - Mag dit eigenlijk wel?
- DPIA
  - Wat zijn de risico's voor betrokkenen?

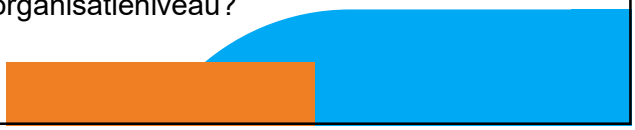


23

INFORMATIE BEVEILIGINGS DIENST

Integrale Risico en Privacy Analyse Informatiebeveiliging

- Baselinetoets:
  - Wat is de maximale schade voor de organisatie?
- Risicoanalyse
  - Wat zijn de risico's voor de organisatie?
- GAP P analyse
  - Welke maatregelen moet ik nemen op procesniveau?
- GAP O analyse
  - Welke maatregelen moet ik nemen op organisatieniveau?



24

INFORMATIE BEVEILIGINGS DIENST

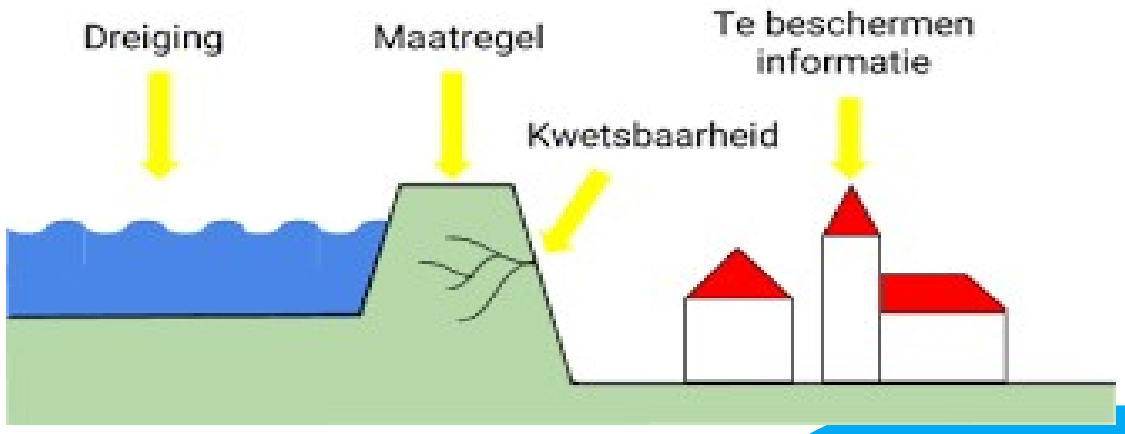
IRPA risicoanalyse methode

- Risico = Kans * Schade.

- Kans-aspect
  - Bepaling voor risicoanalyse en DPIA **dezelfde**.
- Schade-aspect:
  - Bepaling voor risicoanalyse en DPIA **anders**.

25

INFORMATIE BEVEILIGINGS DIENST



26

INFORMATIE BEVEILIGINGS DIENST

Dreigingen

Categorie	Dreiging	Uitleg dreiging	B	I	V
Fysieke schade	Brand	Brand in of bij een locatie	X		
Natuurlijke gebeurtenissen	Overstroming	Van zee, rivier of andere waterweg	X		
Verlies van essentiële diensten	Uitval van openbare telecommunicatieapparatuur	Uitval van openbare telecommunicatieapparatuur	X		
Compromittering van informatie	Afluisteren	Afluisteren of spionage op afstand			X
Technische storingen	Softwarestoring	Software functioneert niet meer volgens de specificaties(dus ook kwetsbaarheden)	X	X	X
Ongeautoriseerde acties	Ongeoorloofd gebruik van apparatuur	Apparatuur gebruiken op een niet toegestane of onveilige manier	X	X	X
Compromitering van functies	Fout in gebruik	Fout in het gebruiken van informatiesystemen	X	X	X
Leverancier of cloud	Scheidingsfouten als gevolg van activiteiten van medegebruikers	Mechanismes falen die zorgen voor het scheiden van opslag, geheugen en routering tussen de verschillende afnemers			X
AVG	AVG rol onduidelijk	Je ziet jezelf als verwerker ipv verantwoordelijke of andersom			X
AVG	Function creep	Functie-uitbreiding waarbij PG voor ander doel verwerkt worden			X
AVG	Geen toestemming betrokkene	Verwerken zonder toestemming betrokkenen terwijl het wel zou moeten			X

27

INFORMATIE BEVEILIGINGS DIENST

Kans

Kans dat een dreiging manifest wordt en één van de **ongewenste scenario's** zich voordoet

De maximale kans wordt binnen IRPA bepaald door drie factoren:

1. De mogelijkheden van de **actoren** en de belangstelling van de actoren voor een bepaald domein/proces.
2. De **dreigingen** die van invloed zijn op het proces.
3. De **kwetsbaarheid** van de productiemiddelen die in het proces worden gebruikt.

28

INFORMATIE BEVEILIGINGS DIENST

Ongewenste scenario's

- Gelijk voor DPIA en Risicoanalyse
  - **Niet beschikbaar** (Verdwijnen) zijn van je proces/Data (B)
  - **Gewijzigd** (Onrechtmatige) kunnen worden van je proces/data (I)
  - **Ingezien** (Onrechtmatige toegang) kunnen worden van je data (V)
- **Restrisico accepteren** door gemeente, dan moet ook onderzocht worden wat **de gevolgen hiervan voor de betrokkenen** zijn.
  - Restrisico voor betrokkenen onacceptabel dan is de beoogde verwerking niet toegestaan.

29

INFORMATIE BEVEILIGINGS DIENST

Schade betrokkenen

Op basis:

- Categorieën persoonsgegevens.
- Bijzondere/gevoelige persoonsgegevens.
- Gegevens van kwetsbare groepen.

Schade reduceren:

- Nemen van specifieke privacy- en informatiebeveiligingsmaatregelen.
  - GAP-O: maatregelen op organisatieniveau
  - DPIA voor de maatregelen op procesniveau

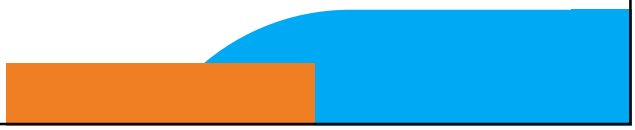
30

INFORMATIE BEVEILIGINGS DIENST

Mogelijke gevolgen betrokkenen.

- Discriminatie
- Schending beroepsgeheim
- Stigmatisering
- Manipulatie
- Financiële schade
- Reputatieschade

- Verlies van controle
- Verlies van zelfstandigheid
- Verlies van eigenwaarde
- Verlies van autonomie
- Verlies van integriteit



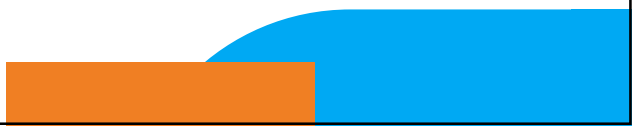
31

INFORMATIE BEVEILIGINGS DIENST

Datalekken

- Een **inbreuk op de beveiliging**, zowel **technisch als organisatorisch** van aard, **waarbij persoonsgegevens betrokken zijn**, is een datalek.
  - Het gaat dan om beveiligingsincidenten waarbij persoonsgegevens **vernietigd**, **verloren zijn gegaan, gewijzigd** of **onrechtmatig zijn verwerkt**, ook wanneer dit **niet redelijkerwijs valt uit te sluiten**.
  - Een beveiligingsincident is géén datalek als er géén persoonsgegevens bij betrokken zijn.

- Voorbeelden:
  - Niet beschikbaar zijn door ransomware
  - Het uitzetten van een verwerking voor log4j



32

INFORMATIE BEVEILIGINGS DIENST

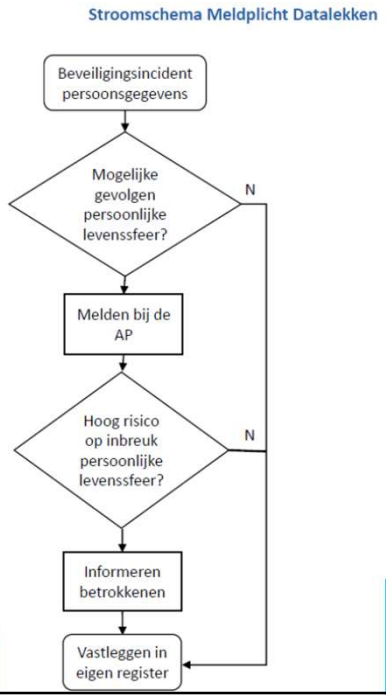
Meldplicht datalekken

Aansprakelijk?

De bestuurder van een gemeente is aansprakelijk voor de eventuele schade die ontstaat bij een datalek en moet hiervan melding te doen.

Wanneer?

Zonder onnodige vertraging en niet later dan 72 uur na de ontdekking, worden gemeld.



INFORMATIE BEVEILIGINGS DIENST

Meldplicht datalekken

- Melden bij:
  - De AP moet geïnformeerd worden bij een datalek.
    - Dit geldt altijd wanneer er persoonsgegevens betrokken zijn bij het incident.
    - Uitzondering is wanneer het niet waarschijnlijk is dat de inbreuk een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.
  - De betrokkene hoeft alleen apart te worden geïnformeerd, wanneer het waarschijnlijk is dat het datalek een hoog risico tot gevolg heeft.

INFORMATIE BEVEILIGINGS DIENST

AVG Borgingsproduct 2.0

- Een hulpmiddel in eerste instantie voor de proceseigenaren om **AVG-controls te implementeren** (organisatiebreed en binnen afdelingen) **en grip te houden** (geen momentopname)
- **Sturingsinformatie** voor het management (ambitieniveau)
- '**Kapstok' document**: privacyproducten aan controls koppelen
- **Vergelijkingen** maken tussen (afdelingen van) gemeenten (gezonde competitie)
- Geen controls die door de BIO worden ingevuld.
  - De verantwoording over de BIO loopt via ENSIA, dus ook de verantwoording over privacy verloopt deels via de ENSIA.

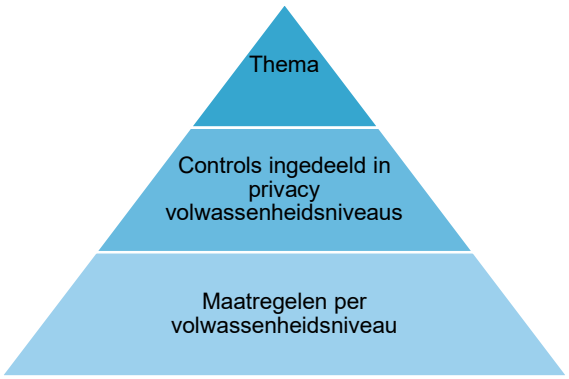
35

INFORMATIE BEVEILIGINGS DIENST

Opbouw

1. Beleid
2. Organisatorische inbedding
3. Processen
4. Rechten van betrokkenen
5. Samenwerking
6. Beveiliging
7. Verantwoording

P en O-maatregelen



36

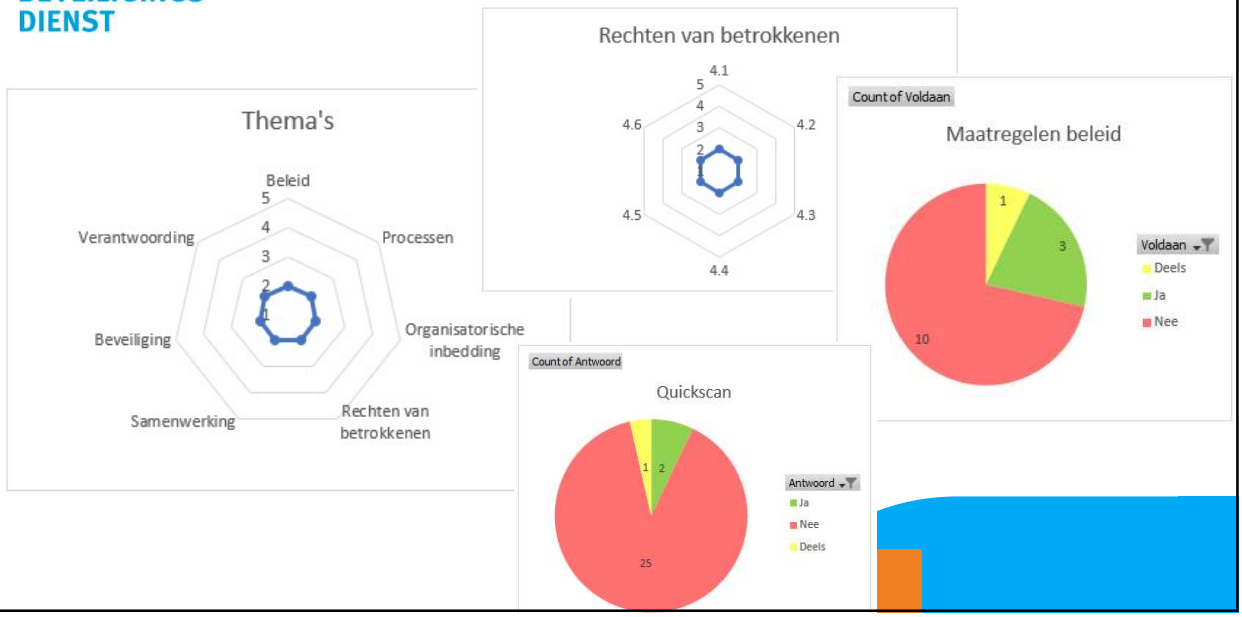
INFORMATIE BEVEILIGINGS DIENST

Voorbeeld thema - beveiliging

Thema	Nr	Control	VN	Omschrijving	Nr	Maatregel	P/O
Beveiliging	6.2	De gemeente heeft inzicht in (potentiële) privacy-incidenten, zoals datalekken.	1	Er zijn weinig tot geen procedures om privacy-incidenten, zoals datalekken, te identificeren en te beheren. Ook is er een tekort aan ondersteuning van privacyspecialisten om privacy-incidenten op te kunnen pakken. Afhankelijk van de individuele expertise en omstandigheden wordt gereageerd.			
			2	Er zijn procedures voor het behandelen van privacy-incidenten, maar het personeel is onvoldoende opgeleid om adequaat te reageren op privacy-incidenten.	20.6.2.1	Medewerkers zijn in grote lijnen op de hoogte van de definitie van een datalek en weten bij wie zij een datalek intern moeten melden.	O
			3	Incidentbeheer is ingericht met gedocumenteerde procedures voor het behandelen van privacy-incidenten. Deze procedures omvatten: identificatie, risicobeoordeling, respons- en escalatie, beheersing, communicatie (aan betrokkenen en de AP), herstel, analyse op de inbreuk, hervatting en verantwoording. Medewerkers zijn hiervan op de hoogte en weten doorgaans hoe ze op een incident moeten reageren.	20.6.2.2	Het is voor medewerkers aantoonbaar duidelijk wanneer sprake is van een (potentieel) datalek.	O

INFORMATIE BEVEILIGINGS DIENST

Grafieken



INFORMATIE BEVEILIGINGS DIENST

Rapportages

- Jaarrapportage / jaarverslag van de FG t.b.v.:
  - Gemeenteraad.
  - College van B&W.
- Inhoud:
  - Terugblik afgelopen jaar
  - Vooruitblik komend jaar
  - Bijlagen:
    - Stand van zaken AVG per thema uit ‘AVG Borgingsproduct 2.0’.
    - Overzicht DPIA’s
    - Overzicht rechten van betrokkenen
    - Overzicht datalekken

39

INFORMATIE BEVEILIGINGS DIENST

Samenwerking FG

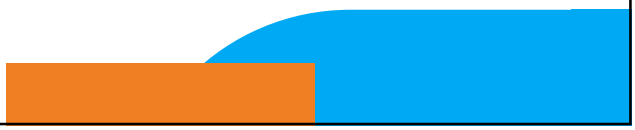
- De interne organisatie
- Het college van B&W en de gemeenteraad
- De ondernemingsraad
- Betrokkenen
- Autoriteit Persoonsgegevens (AP)

40

INFORMATIE BEVEILIGINGS DIENST

(Ondersteunende) taken PO (1/2)

- Opstellen en bijhouden register van verwerkingsactiviteiten
- Opstellen van verwerkersovereenkomsten
- Melding van datalekken

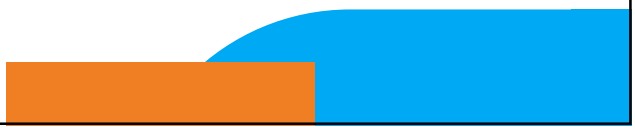


41

INFORMATIE BEVEILIGINGS DIENST

(Ondersteunende) taken PO (2/2)

- Adviseren over de juridische aspecten van de verwerking van persoonsgegevens
- Rechten van betrokkenen
- Ondersteuning bij het opstellen van een DPIA



42

INFORMATIE BEVEILIGINGS DIENST

Samenwerking FG – Chief Information Security Officer

- De taken van de CISO heeft **duidelijke raakvlakken** met de taken van de FG.
- Het aspect '**vertrouwelijkheid van informatie**' behoort immers ook tot het taakgebied van de CISO.
  - Dit geldt trouwens ook voor integriteit en beschikbaarheid!
- Beide rollen kunnen elkaar versterken.
  - Door samen op te trekken bereik je meer!
- FG en CISO **combineren?**
  - Als CISO verantwoordelijk is voor implementeren van informatiebeveiligingsbeleid of aanschaf van ICT systemen?
    - Kan conflicteren met de toezichthoudende rol van de FG en daarvoor vereiste onafhankelijkheid.
  - De AP heeft aangegeven dat het combineren van de CISO en FG rol geen goede combinatie is.

43

INFORMATIE BEVEILIGINGS DIENST

Ondersteuning CISO bij Privacy

- Adviseren over technologie en beveiliging omtrent gegevensverwerking
- Melding van datalekken

44

INFORMATIE BEVEILIGINGS DIENST

Discussiepunten (1/4)

- Hoe zou de Privacyfunctionaris jou (beter) kunnen ondersteunen?
  - Wat ontbreekt er en waarom?
  - In welke situaties zou ik bij je aan moeten kloppen?
  - Gaan informatiebeveiliging en privacy samen naar MT, OR en college? Of ieder voor zich?
  - Gezamenlijk jaarplan informatiebeveiliging en privacy? Waarom wel, waarom niet?
  - Verwerkersovereenkomst verwacht je nog wat van de CISO? Heb ik als CISO hier een rol in?
  - Samen optrekken bij bewustwording?
  - Samen optrekken bij incidenten / datalekken?
- Hoe ziet de taakverdeling er in de praktijk uit? Is deze vastgelegd?

INFORMATIE BEVEILIGINGS DIENST

Discussiepunten (2/4)

- Zijn er momenten waarop de samenwerking niet mogelijk is?
  - Voorbeeld noemen! Tegengestelde belangen!
  - Waar ligt de scheidslijn bij zaken die in het grijze gebied liggen?
- Hoe kunnen we samenwerking optimaliseren?
  - Bijvoorbeeld hoe vaak gaan we gezamenlijk rond de tafel zitten?
- Waar loop je als CISO tegenaan bij je samenwerking met de Privacyfunctionaris?
- Welke privacy basiskennis heeft de CISO nodig om goed samen te kunnen werken?
  - Hoe zie je dat voor je dat de CISO op dat niveau komt? (bijv. Privacy for dummies!)

INFORMATIE BEVEILIGINGS DIENST

Discussiepunten (3/4)

GRC:

- Hebben jullie een Governance, Risk, and Compliance (GRC) tool en worden daar ook privacyrisico's in een vastgelegd?

BCM

- Heeft de FG ook een rol bij bedrijfscontinuïteitsbeheer (BCM) / uitwijk?

Projecten

- Zou je samen op moeten trekken bij de start van een project?
- Hebben jullie een handboek projecten en IB (BIO 6.1.4) en zit daar dan ook privacy in?
- Hoe zorg je ervoor dat informatiebeveiliging en privacy ook bij MT als randvoorwaarde worden benoemd bij de start van een project?
- Hoe wordt je op tijd aangehaakt? Tips!

INFORMATIE BEVEILIGINGS DIENST

Discussiepunten (4/4)

Rapportage bestuur

- Een hulpmiddel om te rapporteren aan directie en bestuur is aan de hand van het volwassenheidsmodel (voor informatiebeveiliging Norea). Voor privacy is er het AVG borgingsproduct 2.0 incl. volwassenheidsmodel. Voor informatiebeveiliging is dit nog niet ontwikkeld.
  - Zijn er gemeenten die hier behoefte aan hebben?
- Hoe vaak en naar wie rapporteer je (manager, MT, Gemeentesecretaris, college, gemeenteraad)?
  - Waarom: omdat je het zelf wil, omdat je het afgesproken hebt, of omdat het je "opgelegd" is?
  - Vorm: mondeling, presentatie, rapportage of combinatie van allen?

INFORMATIE
BEVEILIGINGS
DIENST

Nassaulaan 12
2514 JS Den Haag

CERT: 070 204 55 11 (9:00 – 17:00 ma – vr)
CERT 24x7: Piketnummer (instructies via voicemail)

info@IBDGemeenten.nl / incident@IBDGemeenten.nl