NEMACC voorblad

Informatiebeveiliging & Privacy

- Opdracht NEMACC
- In deze presentatie aandacht voor:
  - Het doorsnee MKB-kantoor
  - Privacywetgeving 2018
- Nu te nemen acties (kantoren / klanten)

De betaalautomaat in Ede met het ransomwarescherm

Foto: Hans van Hoogstrate

Cybersecuritybeeld Nederland 2016

Beroepscriminelen hebben zich ontwikkeld tot geavanceerde actoren en voeren langdurige en hoogwaardige operaties uit

Digitale economische spionage door buitenlandse inlichtingendiensten zet de concurrentiepositie van Nederland onder druk

Ransomware is gemeengoed en is nog geavanceerder geworden

Advertentienetwerken zijn nog niet in staat gebleken malvertising het hoofd te bieden

Vraag

Heeft uw organisatie de laatste 6 maanden een beveiligingsincident gehad?

Een beveiligingsincident kan zijn:

- Een kwijtgeraakte USB-stick
- Een gestolen laptop
- Inbraak door een hacker
- Malware-besmetting
- Verstoring van de verwerking

	Grootte kantoor	
1	0-20	Ja
2	0-20	Nee
3	0-20	Weet niet
4	21-100	Ja
5	21-100	Nee
6	21-100	Weet niet
7	>100	Ja
8	>100	Nee
9	>100	Weet niet

Vraag

Heeft uw organisatie de laatste 6 maanden een datalek gemeld bij de AP?

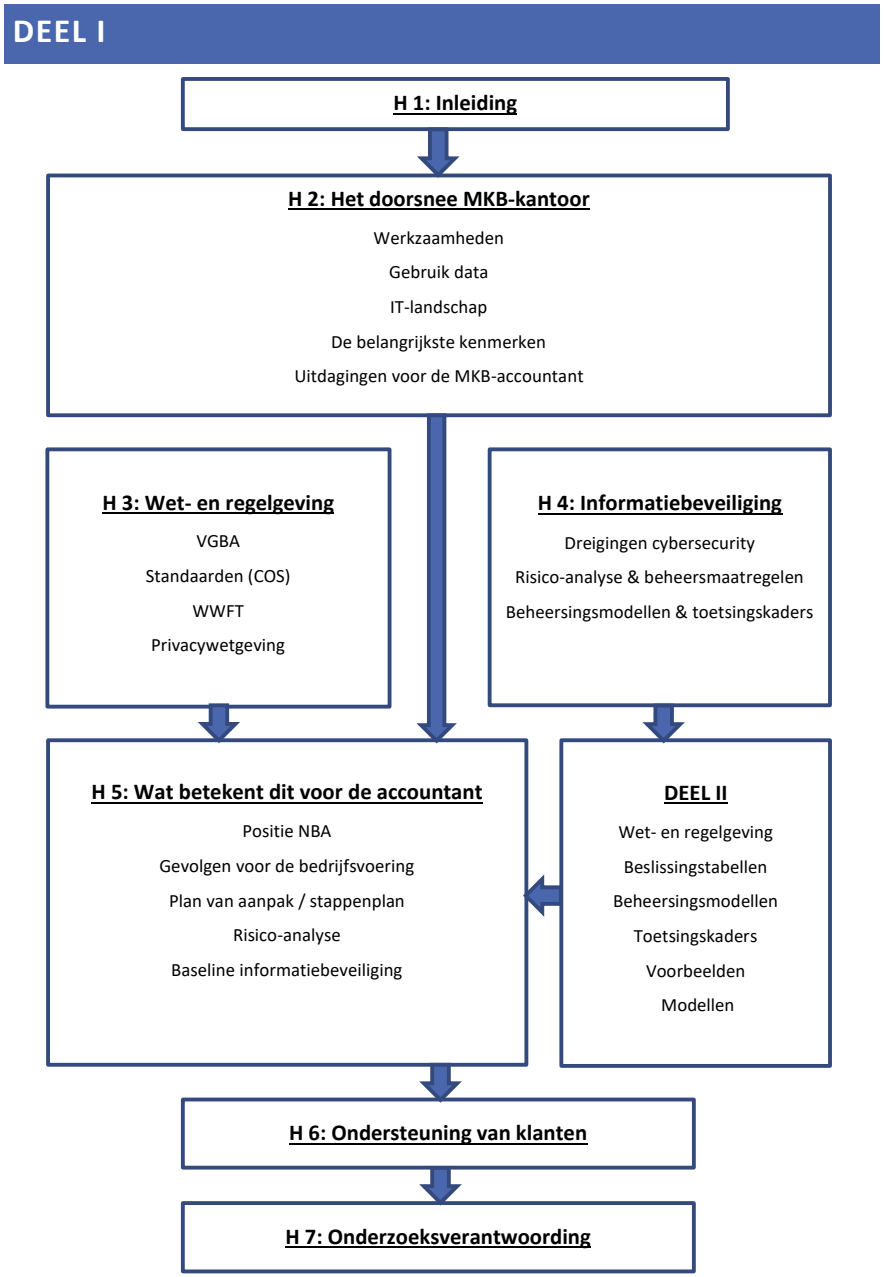
Er is sprake van een datalek als er bij een beveiligingsincident persoonsgegevens verloren zijn gegaan, of als u onrechtmatig gebruik, inzage of verwerking van de persoonsgegevens niet kunt uitsluiten.

	Grootte kantoor	
1	0-20	Ja
2	0-20	Nee
3	0-20	Weet niet
4	21-100	Ja
5	21-100	Nee
6	21-100	Weet niet
7	>100	Ja
8	>100	Nee
9	>100	Weet niet

Opdracht NEMACC

Onderzoeksvragen:

- Welke risico's lopen MKB-accountants op het gebied van datalekken?
- Welke aanpak kan de MKB-accountants ondersteunen in een effectieve databescherming binnen zijn bedrijfsprocessen?
- Welke aanvullende maatregelen moet de MKB-accountant treffen om te voldoen aan de Wet meldplicht datalekken?
- Welke toegevoegde waarde kan de MKB-accountant bieden aan zijn klanten?


DEEL I
H 1: Inleiding
H 2: Het doorsnee MKB-kantoor
Werkzaamheden
Gebruik data
IT-landschap
De belangrijkste kenmerken
Uitdagingen voor de MKB-accountant
H 3: Wet- en regelgeving
VGBA
Standaarden (COS)
WWFT
Privacywetgeving
H 4: Informatiebeveiliging
Dreigingen cybersecurity
Risico-analyse & beheersmaatregelen
Beheersingsmodellen & toetsingskaders
H 5: Wat betekent dit voor de accountant
Positie NBA
Gevolgen voor de bedrijfsvoering
Plan van aanpak / stappenplan
Risico-analyse
Baseline informatiebeveiliging
DEEL II
Wet- en regelgeving
Beslissingstabellen
Beheersingsmodellen
Toetsingskaders
Voorbeelden
Modellen
H 6: Ondersteuning van klanten
H 7: Onderzoeksverantwoording

Het doorsnee MKB-kantoor

- Dienstenpakket
- Mogelijk te gebruiken data
- Applicatielandschap / IT-infrastructuur
- Belangrijke kenmerken
- Actiepunten

Het doorsnee MKB-kantoor

- Als referentiekader voor problematiek
- Mede gebaseerd op interviews met 4 kantoren van verschillende grote en samenstelling
- Feitelijke situatie kan per kantoor verschillen

Overzicht dienstenpakket / werkzaamheden

- Administratieve dienstverlening:
  - Bijhouden van bedrijfsadministraties
  - Personeelsadministratie en salarisverwerking
- Het samenstellen van jaarrekeningen
- Het controleren van jaarrekeningen
- Overige assurance-werkzaamheden
- Fiscale & juridische dienstverlening
- Advisering
- IT-auditing en advisering
- Het aanbieden van online dienstverlening

Overzicht van mogelijk daarbij te gebruiken data

Klantgegevens
Relatie- / contactgegevens - identificerende gegevens van klanten
Notulen / verslagen / correspondentie / e-mailverkeer / berichten sociale media
Plannen: bedrijfsplannen, begrotingen / budgetten; Investeringsplannen
Contractgegevens
CRM-gegevens

HR
Personeels- / salaris- / verzuimgegevens
Reis- / kosten- / zorgdeclaraties

Financieel/administratie
Grootboektransacties;
Investeringen/activa-gegevens
Waarderingen

Fiscaal
Fiscale gegevens (zakelijk en DGA-gegevens);
Juridisch

IT
Passwords, bevoegdheden voor dienstverlening
Koppelingen met derde-partijen

Juridisch
Claims / rechtszaken;
R &D - recepturen / octrooien

Assurance
Bevindingen AO/IC
Rapportages

Advisering
Waarderingen
(mogelijke) Contractspartijen

Data voor bedrijfsvoering

Personeel
Persoonsgegevens
Salarissen
Beoordelingsgegevens
E-mailadressen

IT
Uitbestedingscontracten / SLA's
Gegevens toegangsregelingen
E-mailgegevens

Organisatie
Bevoegheden
Productiegegevens

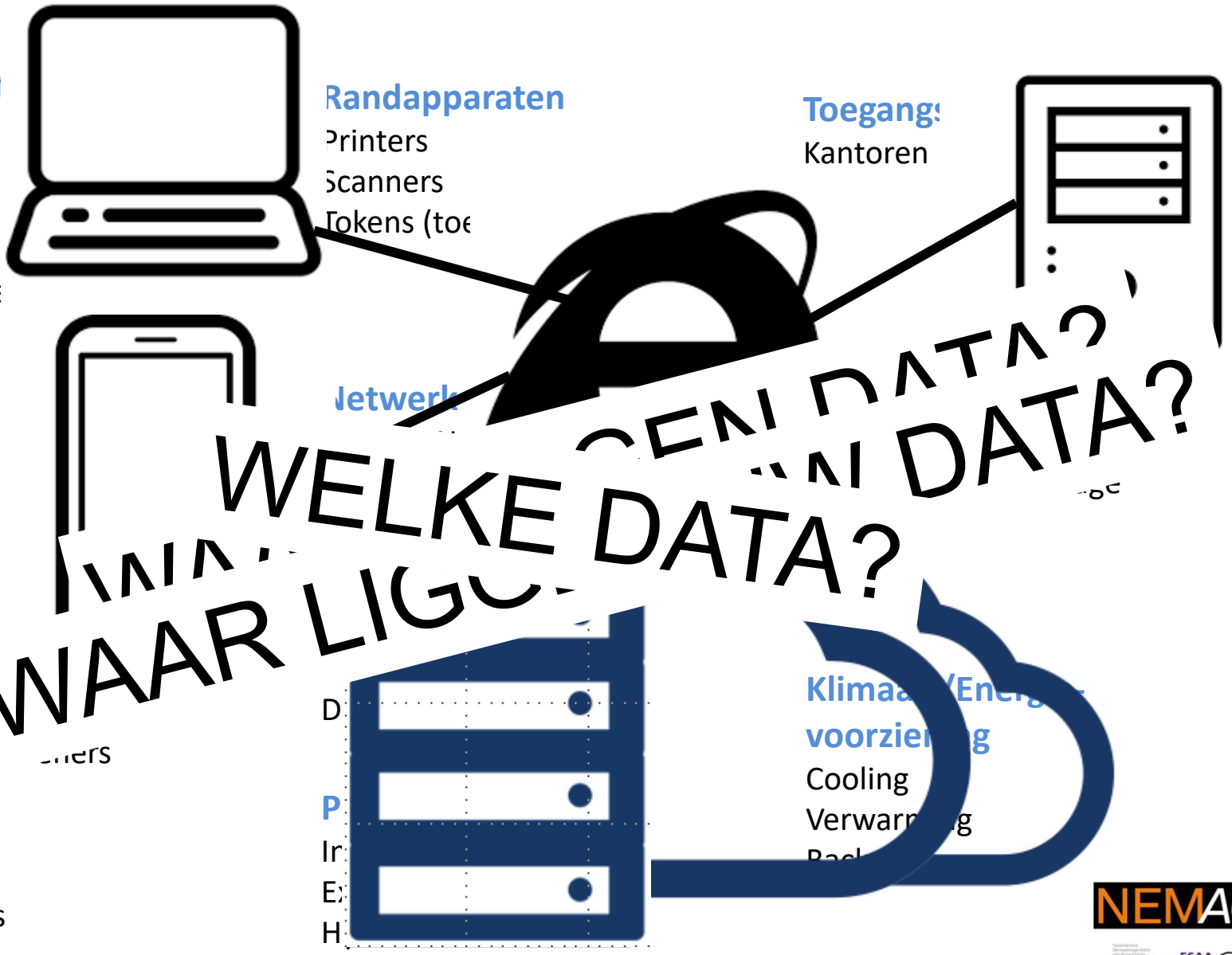
Juridisch
Contracten / -prijzen / -facturen

Financieel
Begrotingen / budgetten
Waarderingen
Aandelen / deelnemingen

Administratie
Kosten en opbrengsten
Debiteuren- / Crediteurengegevens
Betalingen / banktransacties
Prijzen / facturen

Huisv./facilitair
Abonnementen / lidmaatschappen

Organisatie / IT-landschap (infrastructuur)



Gebr.inter
Terminals
PC's
Laptops
Ipads
Smartphone
BYOD

Datacom
Netwerk
Routers/sv
Netwerk f

Uitvoerir
Zelf
Dienstver
Sub-dienst

Backup
Gegevens
Appplicaties

Randapparaten
Printers
Scanners
Tokens (toe

Netwerk

Toegangs
Kantoren

WELKE DATA?

WAAR LIGG

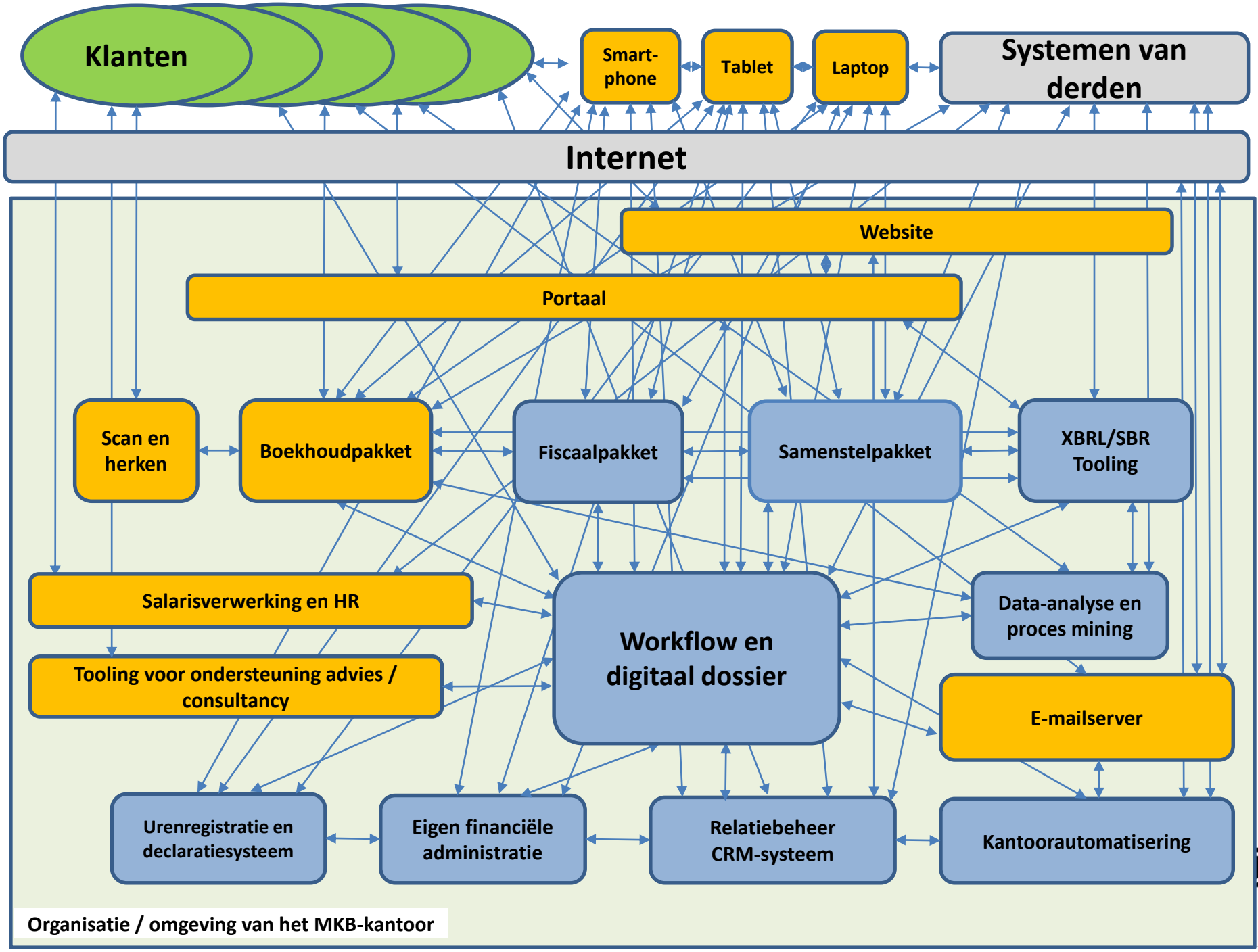
P
Ir
E
H

Klima /Energ
voorzie g
Cooling
Verwar g
Rac

Gegevens accountantskantoor

Bedrijfsvoering **+** **Gegevens Dienstverlening**

Organisatie / IT-landschap


Klanten
Smart-phone
Tablet
Laptop
Systemen van derden
Internet
Website
Portaal
Scan en herken
Boekhoudpakket
Fiscaalpakket
Samenstelpakket
XBRL/SBR Tooling
Salarisverwerking en HR
Workflow en digitaal dossier
Data-analyse en proces mining
Tooling voor ondersteuning advies / consultancy
E-mailserver
Urenregistratie en declaratiesysteem
Eigen financiële administratie
Relatiebeheer CRM-systeem
Kantoorautomatisering
Organisatie / omgeving van het MKB-kantoor

Vraag

Herkent u het geschetste IT- en applicatielandschap?

	Grootte kantoor	
1	0-20	Ja
2	0-20	Nee
3	0-20	Weet niet
4	21-100	Ja
5	21-100	Nee
6	21-100	Weet niet
7	>100	Ja
8	>100	Nee
9	>100	Weet niet

Actiepunten voor nu (voor u en uw klanten)

- Zorg dat medewerkers bewust zijn cyberdreiging (awareness)
- Maak duidelijk afspraken wat wel of niet mag
- Weet met je wie je zaken doet bij het verstrekken van informatie / data
- Start met inventarisatie van huidig dienstenpakket en data
- Breng applicatie- en IT-landschap in kaart, incl. serviceproviders en sub-serviceproviders (derde partijen)
- Maak alleen gebruik van beveiligde verbindingen (ook mobiel)
- Zorg dat (toegangs)beveiliging up to date is, incl. firewalls en patches
- **Maak iemand op bestuursniveau verantwoordelijk**

Wet- en regelgeving

In het kader van informatiebeveiliging en privacywetgeving

- VGBA / WWFT / Privacywetgeving
- Nieuwe privacywet (AVG)
- Belangrijkste bepalingen voor de accountant
- Actiepunten

Beroepsregels

VGBA en WWFT vereisen

- Compliance met regelgeving
- Risico-analyse bedreigingen en toereikende maatregelen gericht op waarborgen **integriteit**, **beschikbaarheid** en **vertrouwelijkheid**
- Cliëntenonderzoek en verificatie van identiteit

Privacywetgeving

WBP
1 september 2001

Meldplicht datalekken
1 januari 2016

AVG
25 mei 2018

Staatsblad
van het Koninkrijk der Nederlanden

Jaargang 2000

302

Wet van 6 juli 2000, houdende regels inzake de bescherming van persoonsgegevens (Wet bescherming persoonsgegevens)

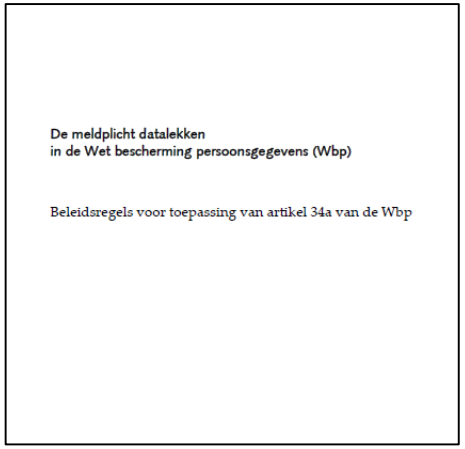
Wij Beatrix, bij de gratie Gods, Koningin der Nederlanden, Prinses van Oranje-Nassau, enz. enz. enz.

Allen, die deze zullen zien of horen lezen, saluut! doen te weten:
Alzo Wij in overweging genomen hebben, dat het noodzakelijk is de richtlijn nr. 95/46/EG van het Europees Parlement en de Raad van de Europese Unie van 23 november 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PbEG L 281) te implementeren;
Gelet op artikel 10, tweede en derde lid, van de Grondwet;
Zo is het, dat Wij, de Raad van State gehoord, en met gemeen overleg der Staten-Generaal, hebben goedgevonden en verstaan, gelijk Wij goedvinden en verstaan bij deze:

HOOFDSTUK 1. ALGEMENE BEPALINGEN

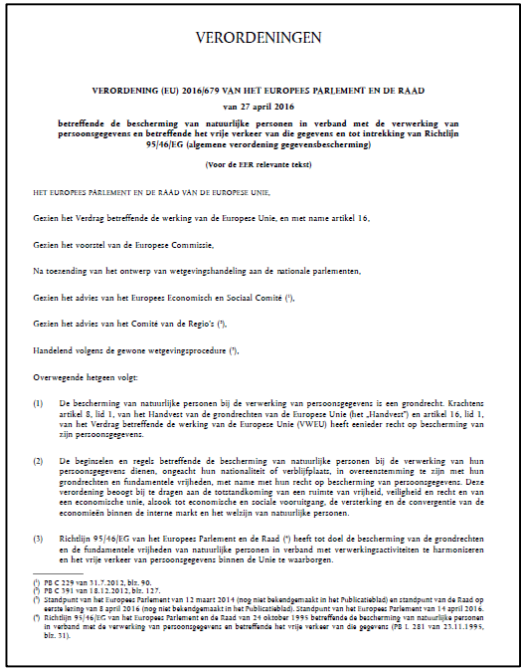
Artikel 1

In deze wet en de daarop berustende bepalingen wordt verstaan onder:
a. persoonsgegeven: elk gegeven betreffende een geïdentificeerde of identificeerbare natuurlijke persoon;
b. verwerking van persoonsgegevens: elke handeling of elk geheel van handelingen met betrekking tot persoonsgegevens, waaronder in ieder geval het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, alsmede het afschermen, uitwissen of vernietigen van gegevens;
c. bestand: elk gestructureerd geheel van persoonsgegevens, ongeacht of dit geheel van gegevens gecentraliseerd is of verspreid is op een functioneel of geografisch bepaalde wijze, dat volgens bepaalde criteria toegankelijk is en betrekking heeft op verschillende personen;
d. verantwoordelijke: de natuurlijke persoon, rechtspersoon of ieder ander die of het bestuursorgaan dat, alleen of te zamen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt;
e. bewerker: degene die ten behoeve van de verantwoordelijke



De meldplicht datalekken
in de Wet bescherming persoonsgegevens (Wbp)

Beleidsregels voor toepassing van artikel 34a van de Wbp



VERORDENINGEN

VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD
van 27 april 2016
betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)

(Voor de EER relevante tekst)

HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie, en met name artikel 16,

Gezien het voorstel van de Europese Commissie,

Na toezending van het ontwerp van wetgevingshandeling aan de nationale parlementen,

Gezien het advies van het Europees Economisch en Sociaal Comité (1),

Gezien het advies van het Comité van de Regio's (2),

Handelend volgens de gewone wetgevingsprocedure (3),

Overwegende hetgeen volgt:

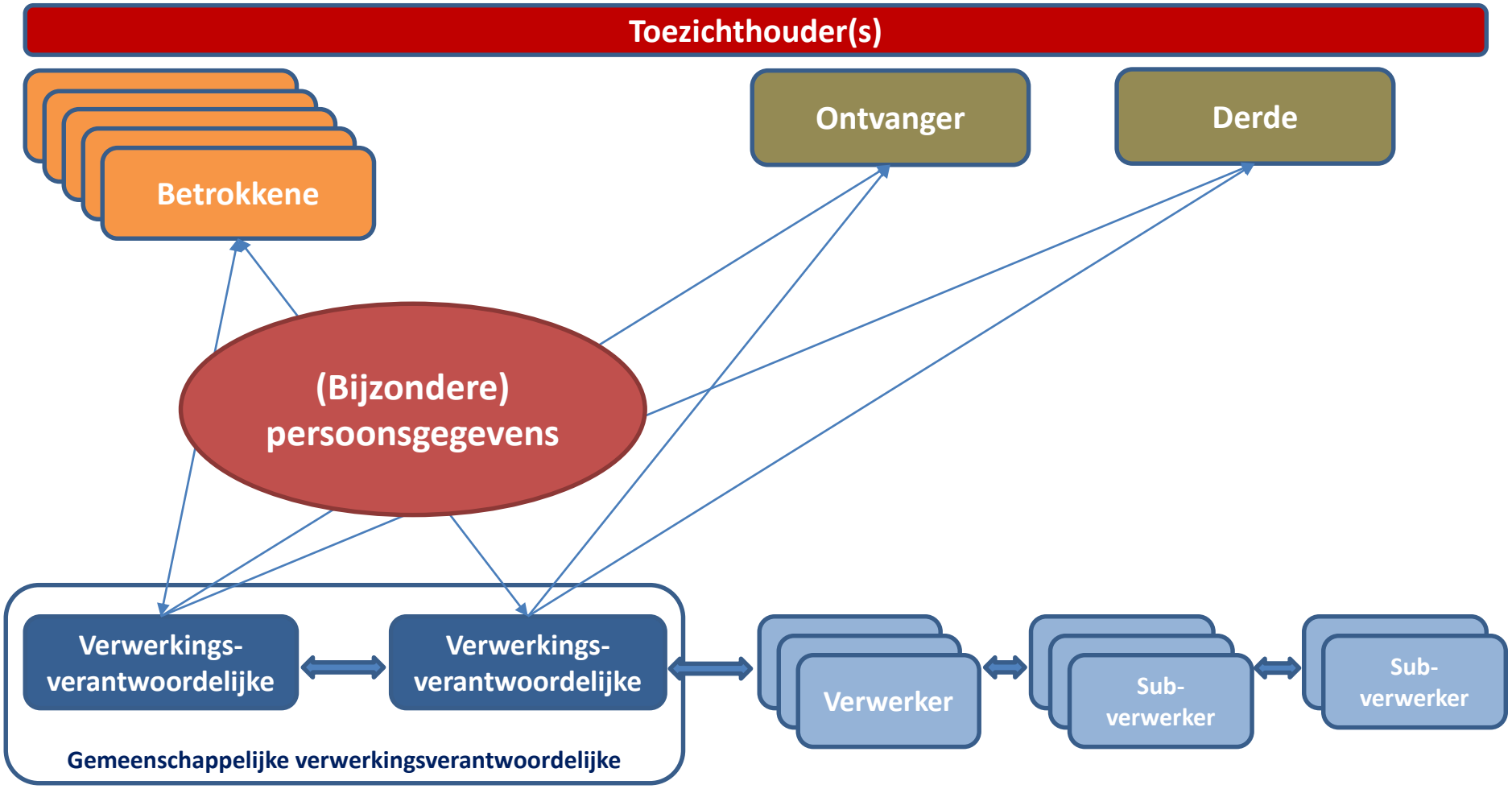
(1) De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht. Krachtens artikel 8, lid 1, van het Handvest van de grondrechten van de Europese Unie (het „Handvest") en artikel 16, lid 1, van het Verdrag betreffende de werking van de Europese Unie (VWEU) heeft eenieder recht op bescherming van zijn persoonsgegevens.

(2) De beginselen en regels betreffende de bescherming van natuurlijke personen bij de verwerking van hun persoonsgegevens dienen, ongeacht hun nationaliteit of verblijfplaats, in overeenstemming te zijn met hun grondrechten en fundamentele vrijheden, met name met hun recht op bescherming van persoonsgegevens. Deze verordening beoogt bij te dragen aan de totstandkoming van een ruimte van vrijheid, veiligheid en recht en van een economische unie, alsook tot economische en sociale vooruitgang, de versterking en de convergentie van de economieën binnen de interne markt en het welzijn van natuurlijke personen.

(3) Richtlijn 95/46/EG van het Europees Parlement en de Raad (4) heeft tot doel de bescherming van de grondrechten en de fundamentele vrijheden van natuurlijke personen in verband met verwerkingsactiviteiten te harmoniseren en het vrije verkeer van persoonsgegevens binnen de Unie te waarborgen.

(1) PB C 229 van 31.7.2012, blz. 90.
(2) PB C 391 van 18.12.2012, blz. 127.
(3) Standpunt van het Europees Parlement van 12 maart 2014 (nog niet bekendgemaakt in het Publicatieblad) en standpunt van de Raad op eerste lezing van 8 april 2016 (nog niet bekendgemaakt in het Publicatieblad). Standpunt van het Europees Parlement van 14 april 2016.
(4) Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens (PB L 281 van 23.11.1995, blz. 31).

Betrokken partijen



Vraag

Bent u op de hoogte van de inhoud van de nieuwe wetgeving per 25 mei 2018?

	Grootte kantoor	
1	0-20	Ja
2	0-20	Nee
3	0-20	
4	21-100	Ja
5	21-100	Nee
6	21-100	
7	>100	Ja
8	>100	Nee
9	>100	

Belangrijkste veranderingen AVG

- Sterkere positie betrokkene
  - Recht op vergetelheid
  - Recht op overdraagbaarheid van gegevens
- Striktere eisen aan verwerkingsverantwoordelijke en (sub-)verwerkers
- Wet vereist passende beveiliging (technische en organisatorische maatregelen)
- Risico-analyse, evaluatie en monitoring verplichte onderdelen beveiliging
- **Naleving van de wet moet kunnen worden aangetoond**
- Wet gaat uit van Privacy by design en by default
- Privacy Impact Analyse / PIA bij nieuwe technologie / verwerkingen verplicht
- Verplichting tot het registreren van verwerkingen (> 250 medewerkers)
- Functionaris gegevensbescherming verplicht (> 250 medewerkers)
- Geleden schade moet worden vergoed
- Hogere boetes: max 20 miljoen of 4% van de wereldwijde omzet

Vraag

Is uw organisatie al gestart met de voorbereiding op de nieuwe wet (AVG)?

	Grootte kantoor	
1	0-20	Ja
2	0-20	Nee
3	0-20	Weet niet
4	21-100	Ja
5	21-100	Nee
6	21-100	Weet niet
7	>100	Ja
8	>100	Nee
9	>100	Weet niet

Belangrijke punten voor de accountant (klant)

Striktere eisen aan verwerkingsverantwoordelijke / (sub)verwerkers

- Alleen gebruik van (sub-)verwerker met toestemming van verwerkingsverantwoordelijke
- Schriftelijke overeenkomst verplicht tussen verwerkingsverantwoordelijken en (sub-)verwerkers
- Verwerker verantwoordelijk voor werkzaamheden sub-verwerker
- Verwerkingsverantwoordelijke:
  - is partij die bij inbreuken op de beveiliging moet melden aan de AP, eventueel aan betrokkene(n)
  - moet alle inbreuken (gemelde en niet gemelde) op beveiliging documenteren, incl. gevolgen en getroffen maatregelen
  - moet dus met (sub-)verwerkers afspraken maken om verplichtingen inzake melding na te kunnen komen
- Melding aan AP vereist aanleveren diverse gegevens m.b.t. de inbreuk, eventuele gevolgen en genomen acties

NBA voert overleg met AP over de rol en positie van de accountant in het kader van zijn werkzaamheden (verwerkingsverantwoordelijke of verwerker).

Vraag

Heeft uw organisatie al een duidelijke procedure m.b.t. het melden van datalekken?

Procedure omvat o.m.:

- persoon aan wie intern moet worden gemeld
- beschikbaarheid van die persoon
- bevoegdheid maar ook de mogelijkheden om afweging te kunnen maken wel of niet melden
- beschikbaarheid van gegevens die in de melding moeten worden opgenomen
- analyse of ook aan betrokkene(n) moeten worden gemeld

	Grootte kantoor	
1	0-20	Ja
2	0-20	Nee
3	0-20	Weet niet
4	21-100	Ja
5	21-100	Nee
6	21-100	Weet niet
7	>100	Ja
8	>100	Nee
9	>100	Weet niet

Actiepunten voor nu (voor u en uw klanten)

- Aanwijzen op bestuurlijk niveau van verantwoordelijke voor informatiebeveiliging / compliance met privacywetgeving (is niet de Compliance Officer)
- Opstarten project om tijdig gereed te zijn voor 25 mei 2018 (vereist o.m. betrokkenheid van IT, HR, Juridische zaken, Compliance)
- Procedure om een datalek te kunnen melden
- Inventarisatie van het gebruik van (bijzondere) persoonsgegevens
- ……..