PELLICAAN

ADVOCATEN & ADVISEURS

Privacy-proof zaken doen!

Kennissessie 6 juni 2017

PELLICAAN

ADVOCATEN & ADVISEURS

Over Pellicaan Advocaten

- Ondernemend kantoor
- Circa 20 advocaten en adviseurs
- Juridisch partner én klankbord voor onze cliënten
- Strategische alliantie met Mazars
- Marcalliance

Privacy-team Pellicaan Advocaten

Xander Alders
088 627 22 87
xander.alders@pellicaan.nl

Elif Barioglu
088 627 22 87
elif.barioglu@pellicaan.nl

Jeroen Belderok
088 627 22 87
jeroen.belderok@pellicaan.nl

Alexander den Hollander
088 627 22 20
alexander.denhollander@pellicaan.nl

Caro Mennen
088 627 22 60
caro.mennen@pellicaan.nl

Ellen Timmer
088 627 22 87
ellen.timmer@pellicaan.nl

Privacy-proof zaken doen!

Privacyrecht

PELLICAAN
ADVOCATEN & ADVISEURS

Privacyrecht

Geschiedenis

- 1988 – Wet persoonsregistraties
- 2001 – Wet bescherming persoonsgegevens (Wbp) / Privacyrichtlijn 95/46/EG
- 2016 – Wet meldplicht datalekken
- 2018 – Algemene verordening gegevensbescherming (AVG)

What's new?

- Uitgangspunten uit de Wbp zijn onveranderd – open normen
- Nieuwe verplichtingen en meer gedetailleerde uitwerking
- Meer rechten voor betrokkenen
- Uitbreiding reikwijdte
- Hoge(re) boetes

PELLICAAN

Begrippen

(Verwerkings)verantwoordelijke

Stelt alleen of tezamen met anderen het doel en de middelen voor de verwerking van persoonsgegevens vast

Verwerker
Degene die ten behoeve van de verantwoordelijke persoonsgegevens verwerkt zonder aan zijn rechtstreeks gezag te zijn onderworpen

Betrokkene
Degene op wie een persoonsgegeven betrekking heeft

Verwerking
Elke handeling of geheel van handelingen met betrekking tot persoonsgegevens

PELLICAAN

Persoonsgegeven?

- naam
- telefoonnummer
- postcode
- kenteken van een motorvoertuig
- IP-adres
- inlognamen
- geluids- en video-opnamen
- foto's
- winst

Persoonsgegeven
Elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon

Bijzondere persoonsgegevens
Persoonsgegevens betreffende ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap vakbond, genetische gegevens, biometrische gegevens met het oog op identificatie, gezondheid, seksueel gedrag of seksuele gerichtheid

PELLICAAN

Doelbinding

Voor welk(e) doeleinde(n) vindt de verwerking plaats?

- Welbepaald
- Ondubbelzinnig
- Gerechtvaardigd

[Wij] verwerken uw persoonsgegevens voor de volgende doeleinden:

- voor het uitvoeren van de overeenkomst die wij met u hebben gesloten
- voor het versturen van gepersonaliseerde berichten die aansluiten bij uw interesses
- voor het versturen van informatie over nieuwe producten of diensten
- om te kunnen voldoen aan de op ons rustende wettelijke verplichtingen

PELLICAAN

Waar?! Niet waar?!

Betrokkenen moeten toestemming geven voor het verwerken van hun persoonsgegevens

A. Waar
B. Niet waar

PELLICAAN

Rechtmatige verwerking

Grondslag voor verwerking:

- Uitvoeren overeenkomst met de betrokkene
- Wettelijke verplichting van de verantwoordelijke
- Bescherming vitale belangen betrokkene
- Taak van algemeen belang/uitvoering openbaar gezag
- Gerechtvaardigd belang verantwoordelijke

- Toestemming betrokkene

PELLICAAN

Rechten van betrokkenen

Betrokkenen hebben de volgende rechten:

- recht op **inzage**
- recht op **rectificatie**
- recht op (**gegevens)wissing**
- recht op **beperking** van de verwerking
- recht op overdraagbaarheid van gegevens (**dataportabiliteit**)
- recht van **bezwaar**

PELLICAAN

Privacy principes

Ø **Transparantie**
- Informeer op een heldere en duidelijke manier

Ø **Minimale gegevensverwerking**
- Toereikend, ter zake dienend en noodzakelijk voor doeleinden

Ø **Opslagbeperking**
- Niet langer dan noodzakelijk voor doeleinden

Ø **Juistheid – actualisatie**
- Voorkomen dat onjuiste gegevens worden verwerkt, rectificatie en wissen

Ø **Integriteit & vertrouwelijkheid**
- Passende technische en organisatorische beveiligingsmaatregelen

Ø **Verantwoordingplicht (accountability)**
- Naleving van de AVG moet aantoonbaar gemaakt worden door de verantwoordelijke

PELLICAAN

Verplichtingen[1]

Register van gegevensverwerkingen

Wie?	Verantwoordelijke en verwerker
Wat?	Een register van de (categorieën van) verwerkingsactiviteiten
Hoe?	In schriftelijke vorm waaronder elektronisch
Waarom?	Accountability, op verzoek Autoriteit Persoonsgegevens wordt het register ter beschikking gesteld.
Wanneer niet?	< 250 personen in dienst tenzij: • risicovolle verwerkingen; of • structurele verwerking van persoonsgegevens; of • verwerking van gevoelige persoonsgegevens

PELLICAAN

Verplichtingen[2]

Informeren van betrokkenen

Wie?	Verantwoordelijke
Wat?	Informeren van de betrokkene over verwerkingen en diens rechten
Wanneer?	i.b. bij het verkrijgen van de persoonsgegevens
Wanneer niet?	- de betrokkene beschikt al over de informatie; *Indien gegevens niet rechtstreeks van de betrokkene worden verkregen ook niet indien:* - registratie of mededeling is uitdrukkelijk voorgeschreven bij wet; - informatieverstrekking is onmogelijk of vraagt onevenredig veel inspanning; - geheimhouding i.h.k.v. beroepsgeheim.
Waarom?	Transparantie, vaak via privacy statement

PELLICAAN

Verplichtingen[3]

Gegevensbeschermingseffectbeoordeling / Privacy impact assessment (PIA)

Wie? Verantwoordelijke

Wat? Instrument waarmee privacyrisico's van bepaalde verwerkingen in kaart worden gebracht

Wanneer? Voorafgaand aan de verwerking als waarschijnlijk is dat verwerking vanwege aard, omvang, context en doeleinden een hoog risico voor rechten en vrijheden natuurlijke personen oplevert.

In ieder geval indien:

- er systematische en uitvoerige beoordeling van persoonlijke aspecten van personen, waaronder profiling, plaatsvindt;
- er op grote schaal bijzondere persoonsgegevens worden verwerkt;
- er op grote schaal en systematisch mensen worden gemonitord in een voor publiek toegankelijk gebied;
- AP komt met een lijst met andere verplichte situaties.

Waarom? Accountability, conclusie PIA:

- hoog risico voor rechten en vrijheden van personen?
- risico's niet te beperken door redelijke maatregelen verantwoordelijke? à raadpleging AP.

PELLICAAN

Verplichtingen[4]

Functionaris voor de gegevensbescherming
(Data Protection Officer/DPO)

Wie?	Verantwoordelijke en verwerker
Wat?	Interne toezichthouder die binnen een onderneming onafhankelijk toezicht houdt op het verwerken van persoonsgegevens
Wanneer?	Vrijwillig of verplicht indien: • Overheidsinstantie of -orgaan; • Op grote schaal bijzondere persoonsgegevens worden verwerkt en dit een kernactiviteit is; • Op grote schaal personen regelmatig en stelselmatig worden geobserveerd en dit een kernactiviteit is.

Best practices

Please do ~~not~~ try this at ~~home~~ your company

- ü Inventariseer, maak keuzes en beleid
- ü Zorg dat de IT up-to-date is en aansluit op beleid
- ü Bewustwording bij uw medewerkers/collega's
- ü Need-to-know access
- ü Privacy by design
- ü Privacy by default

DIGITAL ASSURANCE IN EEN CYBER TIJDPERK

Frank Baalbergen Mazars Management Consultants

EVEN VOORSTELLEN

Frank Baalbergen CISSP | Manager Cyber Security

§ 7 jaar ervaring als System and Network Engineer & DevOps Engineer bij Mendix

§ Sinds 2,5 jaar werkzaam als Cyber Security specialist bij Mazars (o.a. uitvoeren van Penetratietesten)

§ Expertise op het gebied van:
- § Web applicatie security
- § Ethical Hacking / Penetratietesten
- § Programmeren & Source code analysis

Mazars Center of Excellence IT-audit en –advisory (sinds 1981)

REAL FUTURE

§ What Happens When You Dare Expert Hackers To Hack You

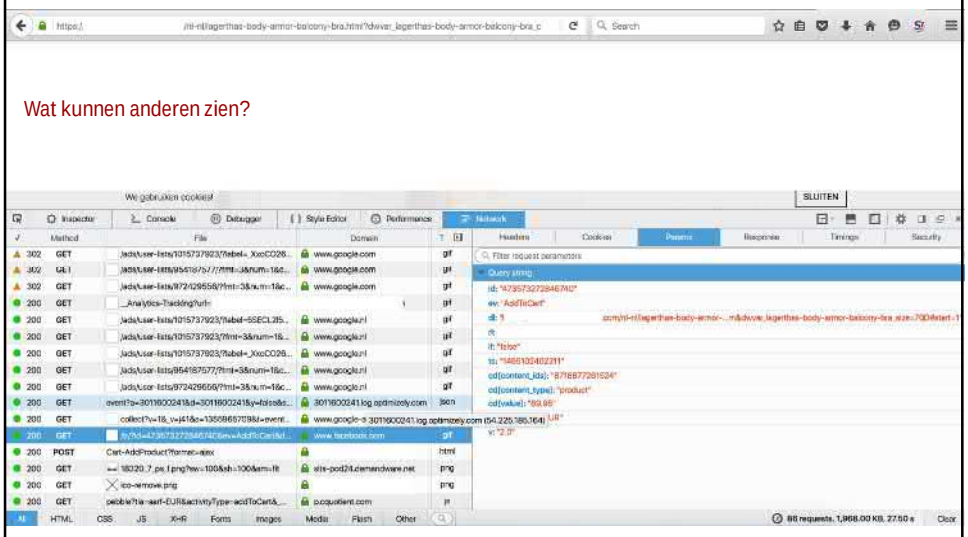
§ https://www.youtube.com/watch?v=zlRMVgYnCrc

VOORBEELDEN

Geen/onvoldoende inzicht in effectiviteit maatregelen

- Wat zien wij tijdens onze penetratietesten:
  - Productiewachtwoorden in design documenten
  - Bekend salarissysteem i.c.m. error logging module a.g.v. een zero day
  - Telefooncentrale gehackt, waardoor torenhoge rekeningen
  - Lingerie maten verstuurd naar derden

MAZARS



Wat kunnen anderen zien?

- Stel je eens voor dat een twitter campagne gestart wordt.

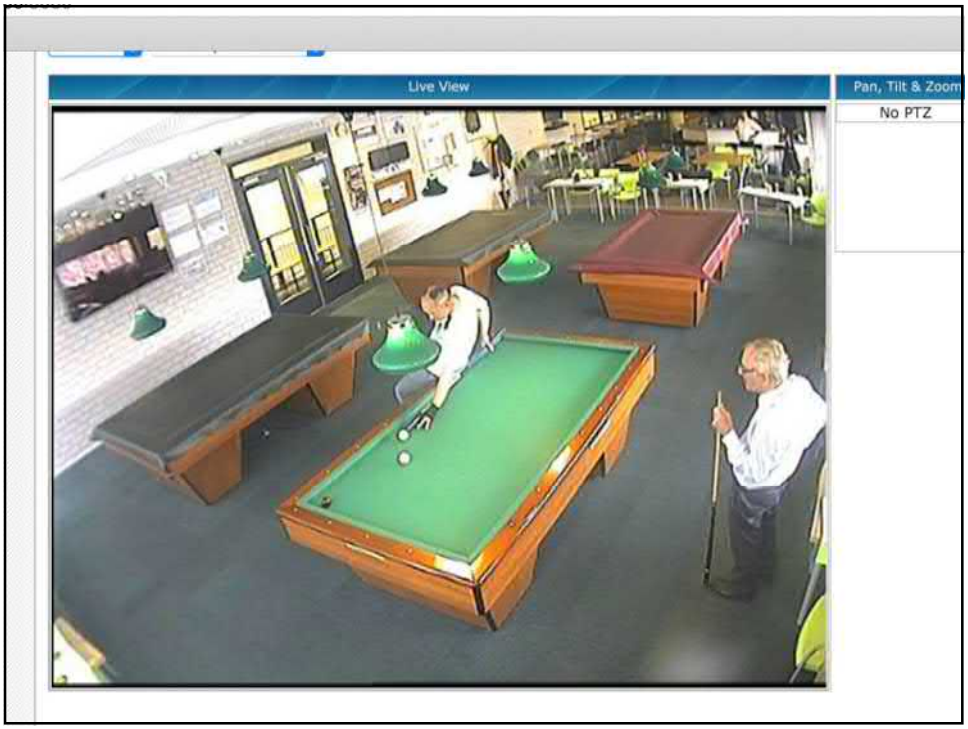
MAZARS

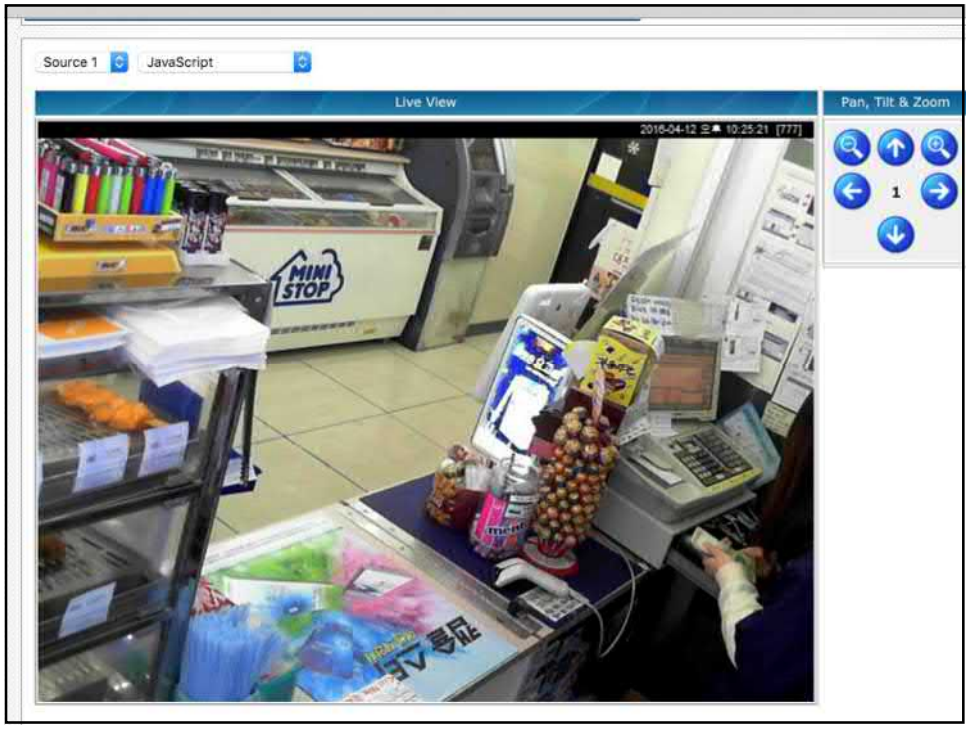
ZOEKMACHINE VOOR ALLES - IOT

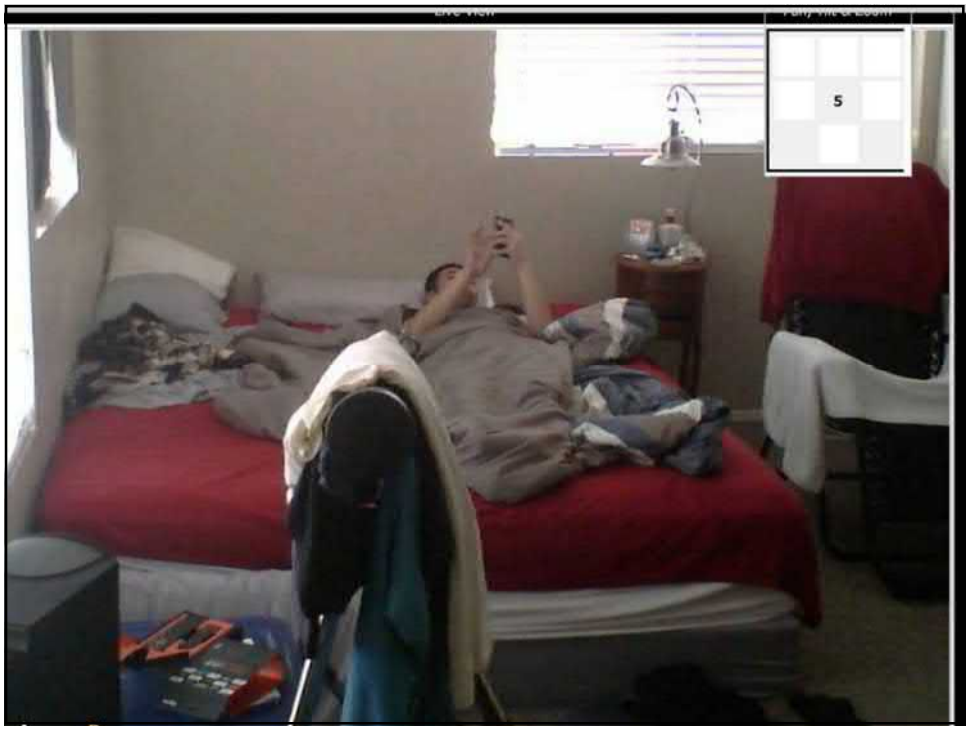
Wat kunnen anderen zien?

§ Microsoft IIS/5.0: 79,325
§ Microsoft IIS/6.0: 1,000,139
§ Webcams: 2000+

§ https://shodan.io
  § Koelkasten
  § Auto's
  § En webcams……




Source 1
JavaScript
Live View
Pan, Tilt & Zoom
2016-04-12 오후 10:25:21 [777]
MINI STOP
1


5

From:
Sent: Saturday, January 30, 2016 4:43 AM
To:
Subject: Let op! Uw digitale handtekening

Wij van het team secure en protect hebben een nieuwe beveiligingsmethode uitgevonden om onze klanten te beschermen.

De "Digitale Handtekening", deze beveiligingsmethode zal ervoor zorgen dat derden geen toegang meer kunnen verschaffen tot uw rekening.

Uit voorzorgsmaatregelen hebben wij uw rekening op echter non-actief gezet tot dat u de "Digitale Handtekening" activeert.

"Digitale Handtekening" Activatie Procedure"

Het niet activeren van de "Digitale Handtekening" zal er voor zorgen dat u geen betaling kan maken met uw betaalpas.

Wij verzoeken u echter om deze procedure te activeren **binnen 24 UUR** om vandaag nog gebruik te maken van uw betaalpas(sen).

Wij danken u voor uw medewerking aan het proces.

ABN·AMRO

29

MAZARS

From: CJIB
Sent: Thursday, March 10, 2016 6:55 AM
To:
Subject: Openstaande aanmaning voorkom een verhoging

Centraal Justitieel Incassobureau
Ministerie van Veiligheid en Justitie

Betreft: Laatste aanmaning inzake
Referentie: 45S2XSPL1

Geachte bestuurder,

Bij deze willen wij u mededelen dat u nog een bedrag bij ons heeft openstaan wegens het overtreden van een verkeersvoorschrift, hoewel de betalingstermijn reeds is overschreden.
Hiervoor heeft u al twee aanmaningen ontvangen.
Het openstaande bedrag van **€ 103,50-**, (incl. kosten) is tot op heden **niet** volledig op de rekening van het CJIB bijgeschreven.

Informatie over de overtreding en de opgelegde administratieve sanctie:

Omschrijving overtreding:	Overschrijding maximum snelheid op autosnelwegen, **niet 14 km/h**
Datum:	9 Januari 2016
Toegestaande snelheid:	100 km/h
Gemeten snelheid:	114 km/h
Gecorrigeerde snelheid:	110 km/h
Zaaknummer:	B118126
Openstaande bedrag:	€ 86,00-,
Administratiekosten:	€ 4,00-,
Incassokosten:	€ 10,00-,
Te betalen:	**€ 100,00-**
3v Aankooptoeslag:	**€ 3,50-,**
Totaal:	€ 103,50

Bedrag en specificaties:

Het gaat hierbij om dat u bent geflits met een snelheid van 14 km/h te hard op de snelweg.
Het verschuldig bedrag kunt u uitsluitend alleen nog betalen via de betaaloptie 3v payment u kunt de betaling via ideal direct uitvoeren via de onderstaande betaal link.

Klik hier om het verschuldigt bedrag direct via ideal te betalen.

Wij hopen echter dat u voor een tijdige betaling zorgt en dat we hiermee de incasso maatregel achterwegen kunnen laten.

Mochten wij uw betaling niet op tijd ontvangen zijn wij genoodzaakt het verschuldigde bedrag te verhogen.

Hoogachtend

Centraal Justitieel Incassobureau.

MAZARS

CYBER SECURITY

OORZAKEN

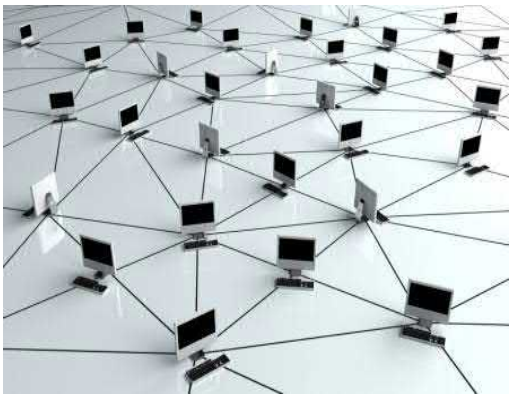
Patch Management

§ Systemen / infrastructuur te complex om snel / eenvoudig te patchen

§ Legacy systemen (geen ondersteuning meer)

§ ‘Als het werkt, niet aan zitten!’

§ Patchen kost tijd (en geld) à dus lage frequentie



MAZARS

VOORBEELDEN

Patch Management

§ Recent: **WannaCry ransomware**

§ Lek in Windows ontdekt door NSA (en geheimgehouden)
- § Update uitgebracht door Microsoft op 14 maart 2017

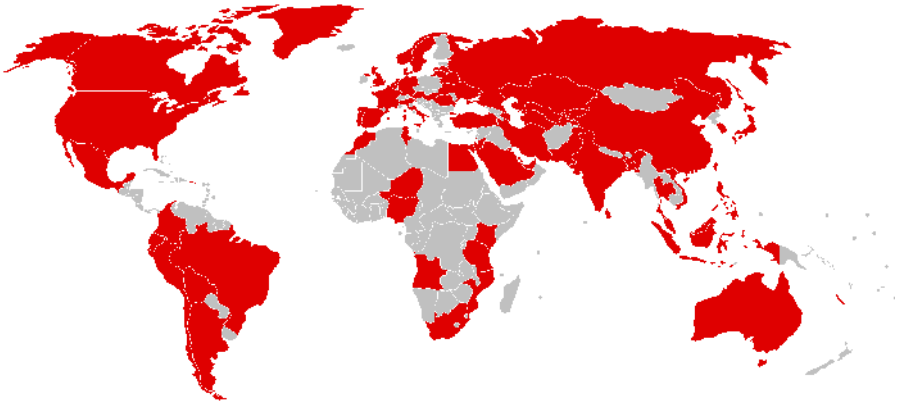
§ 230.000 computers besmet in 150 landen binnen een paar dagen
- § Ransomware was vertaald naar 28 (!) talen
- § Versleuteld al je bestanden en vraagt $ 300 - $ 600 in Bitcoins

§ Grotere slachtoffers:
- § Diverse ziekenhuizen in Engeland (NHS)
- § Q-Park (NL)

VOORBEELDEN

Patchmanagement

§ Geïnfecteerde landen WannaCry



MAATREGELEN

§ Richt patchmanagement in, draai Windows updates.
§ Compartimenteer het netwerk net zoals bij een schip.
§ Richt configuratiemanagement in van servers.
§ Wees strikt op interne en vooral op externe firewalls.

§ Voer externe security scans uit.
§ Test uw eigen websites met https://ssllabs.com
§ Vraag een TPM op bij leveranciers.
§ Laat user awareness trainingen uitvoeren.

WAAR KAN MAZARS U MEE HELPEN?

§ IT audits, TPM's, UWV audits, DigiD audits en Suwinet audits.

§ Externe en interne security scans uitvoeren.

§ User awareness trainingen uitvoeren zoals phishing campagnes.

§ Privacy Impact Assessments & GDPR assessments.

§ Potentieel datalek onderzoek.

§ Compliancy checker i.s.m. Eset. https://www.eset.com/nl/compliance-check/

Privacy-proof zaken doen!

HANDHAVING

PELLICAAN
ADVOCATEN & ADVISEURS

Handhaving - Beleid en jaarverslag AP 2016

1. Beveiliging & meldplicht datalekken
2. Big data & profiling
3. Medische gegevens
4. Persoonsgegevens bij de (digitale) overheid
5. Persoonsgegevens in de arbeidsrelatie

PELLICAAN
ADVOCATEN & ADVISEURS

Handhaving - Beleid AP 2017[1]

1. Nieuwe Europese Privacywetgeving
2. Profiling
3. Bijzondere persoonsgegevens
4. Beveiliging van persoonsgegevens

PELLICAAN
ADVOCATEN & ADVISEURS

Handhaving - Beleid AP 2017[2]

1. Nieuwe Europese Privacywetgeving

- Voorlichting en advisering over AVG, onder meer:
  - Implementatie verplichtingen AVG
  - Bevoegde autoriteit
  - Dataportabiliteit
- E-privacy verordening

PELLICAAN
ADVOCATEN & ADVISEURS

Handhaving - Beleid AP 2017[3]

2. Profiling

- Big data analyses
- Gegevensknooppunten
- Koppeling online en offline data

à Invloed op keuzevrijheid en ontwikkeling van betrokkenen?
à Focus op transparantie

PELLICAAN
ADVOCATEN & ADVISEURS

Handhaving - Beleid AP 2017[4]

3. Bijzondere persoonsgegevens

- Invloed big data en profiling;
- Doelbinding;

à Handhaving verbod verwerking van bijzondere persoonsgegevens

à Juiste toepassing uitzonderingen op het verbod

PELLICAAN
ADVOCATEN & ADVISEURS

Handhaving - Beleid AP 2017[5]

4. Beveiliging van persoonsgegevens

- Opkomst klantenportalen;
- Snelle ontwikkeling nieuwe technologieën;

à Toezicht op beveiliging portalen en andere (nieuwe) technische mogelijkheden

à Toezicht op naleving meldplicht datalekken

à Focus op andere (overduidelijke) beveiligingsrisico's

PELLICAAN
ADVOCATEN & ADVISEURS

Handhaving - Sancties[1]

Handhavingsbevoegdheden Autoriteit:

- Bindende aanwijzing geven (tot aan inwerkingtreding AVG);
- (Administratieve) boete opleggen;

(Na inwerkingtreding AVG:)

- Waarschuwing geven
- Berisping geven
- Diverse bevelen geven
- Verwerkingsverbod opleggen
- Rectificeren of wissen van persoonsgegevens
- Certificeringen (laten) intrekken
- Opschorting doorgifte naar het buitenland
- Last onder bestuursdwang (Uitvoeringswet AVG)

PELLICAAN
ADVOCATEN & ADVISEURS

Handhaving – Sancties[2]

Hoogte van de te geven boetes:

Onder de Wbp
€ 0 - € 820.000 (€ 900.000 ingeval van Telecommunicatiewet) of 10% jaaromzet

Na inwerkingtreding van de AVG
€ 0 - € 10.000.000 of 2% wereldwijde jaaromzet
€ 0 - € 20.000.000 of 4% wereldwijde jaaromzet

PELLICAAN
ADVOCATEN & ADVISEURS

Handhaving – Sancties[3]

Relevante factoren (onder de Wbp):

6.1 De Autoriteit Persoonsgegevens houdt rekening met de ernst van de overtreding. De Autoriteit Persoonsgegevens stemt de beoordeling van de ernst van de overtreding in het concrete geval af op:
a. de aard en omvang van de overtreding;
b. de duur van de overtreding;
c. de impact van de overtreding op (de bescherming van persoonsgegevens en van de persoonlijke levenssfeer voor) de betrokkenen en/of de maatschappij.

6.2 De Autoriteit Persoonsgegevens houdt rekening met de mate waarin de overtreding aan de overtreder kan worden verweten. Indien de overtreding opzettelijk is gepleegd of het gevolg is van ernstig verwijtbare nalatigheid als bedoeld in artikel 66, vierde lid, van de Wet bescherming persoonsgegevens, wordt aangenomen dat sprake is van een aanzienlijke mate van verwijtbaarheid van de overtreder.

6.3 De Autoriteit Persoonsgegevens houdt zo nodig rekening met de omstandigheden waaronder de overtreding is gepleegd en de (financiële) omstandigheden waarin de overtreder verkeert.

PELLICAAN
ADVOCATEN & ADVISEURS

Handhaving – Sancties[4]

Relevante factoren (onder de AVG):

a) de aard, de ernst en de duur van de inbreuk, rekening houdend met de aard, de omvang of het doel van de verwerking in kwestie alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade;

b) de opzettelijke of nalatige aard van de inbreuk;

c) de door de verwerkingsverantwoordelijke of de verwerker genomen maatregelen om de door betrokkenen geleden schade te beperken;

d) de mate waarin de verwerkingsverantwoordelijke of de verwerker verantwoordelijk is gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd overeenkomstig de artikelen 25 en 32;

e) eerdere relevante inbreuken door de verwerkingsverantwoordelijke of de verwerker;

f) de mate waarin er met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;

g) de categorieën van persoonsgegevens waarop de inbreuk betrekking heeft;

h) de wijze waarop de toezichthoudende autoriteit kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke of de verwerker de inbreuk heeft gemeld;

i) de naleving van de in artikel 58, lid 2, genoemde maatregelen, voor zover die eerder ten aanzien van de verwerkingsverantwoordelijke of de verwerker in kwestie met betrekking tot dezelfde aangelegenheid zijn genomen;

j) het aansluiten bij goedgekeurde gedragscodes overeenkomstig artikel 40 of van goedgekeurde certificeringsmechanismen overeenkomstig artikel 42; en

k) elke andere op de omstandigheden van de zaak toepasselijke verzwarende of verzachtende factor, zoals gemaakte financiële winsten, of vermeden verliezen, die al dan niet rechtstreeks uit de inbreuk voortvloeien.

PELLICAAN
ADVOCATEN & ADVISEURS

Handhaving – Sancties[5]

Boete verlagende omstandigheden:

Boeteverlagende omstandigheden zijn in ieder geval:

a. de omstandigheid dat de overtreder verdergaande medewerking aan de Autoriteit Persoonsgegevens heeft verleend dan waartoe hij wettelijk gehouden was;
b. de omstandigheid dat de overtreder uit eigen beweging de overtreding heeft beëindigd voor of bij de eerste bekendwording met het onderzoek van de Autoriteit Persoonsgegevens;
c. de omstandigheid dat de overtreder uit eigen beweging degenen aan wie door de overtreding schade is berokkend, schadeloos heeft gesteld.

Prioriteiten Autoriteit:

a. ernstige overtredingen;
b. structurele overtredingen;
c. overtredingen die veel mensen treffen;
d. overtredingen waarbij het CBP door de inzet van handhavingsinstrumenten effectief verschil kan maken;
e. overtredingen die vallen binnen de (jaarlijkse) aandachtspunten die door het CBP bekend zijn gemaakt.

PELLICAAN
ADVOCATEN & ADVISEURS

Privacy-proof zaken doen!

Wet meldplicht datalekken

PELLICAAN
ADVOCATEN & ADVISEURS

Wet meldplicht datalekken

1. Wat is een datalek?
2. Voorwaarden voor het melden van een datalek bij de AP
3. Inhoud van de melding bij de AP
4. Melden bij betrokkene?
5. Verschillen onder de AVG
6. Voorbeelden van datalekken
7. Overzicht AP feiten en cijfers 1e kwartaal 2017
8. Verwerkersovereenkomst

PELLICAAN
ADVOCATEN & ADVISEURS

Wat is een datalek?

AP:

"We spreken van een datalek als er een inbreuk is op de beveiliging van persoonsgegevens (zoals bedoeld in artikel 13 van de Wet bescherming persoonsgegevens). Bij een datalek zijn de persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking – dus aan datgene waartegen de beveiligingsmaatregelen bescherming moeten bieden."

PELLICAAN
ADVOCATEN & ADVISEURS

Voorwaarden voor het melden van een datalek

- Wanneer moet u melden?
- Vereisten
  - Inbreuk op de beveiliging?
  - Persoonsgegevens verloren gegaan?
  - Valt redelijkerwijs uit te sluiten dat persoonsgegevens onrechtmatig zijn verwerkt?
- Of meldt u niet?
  - Aanzienlijke kans op ernstige nadelige gevolgen voor de bescherming persoonsgegevens?

PELLICAAN
ADVOCATEN & ADVISEURS

‘Niet melden cybercrime is vaak verstandiger’

Advocaat Aldo Verbruggen bekritiseert meldingsplicht bedrijven

Niet melden van datalekken is ‘penny-wise and pound-foolish’

PELLICAAN
ADVOCATEN & ADVISEURS

Inhoud van de melding bij de AP

- Binnen 72 uur melden
- Aard van de inbreuk
- Beschrijving van geconstateerde en vermoedelijke gevolgen van de inbreuk voor de verwerking van persoonsgegevens
- Genomen maatregelen

PELLICAAN
ADVOCATEN & ADVISEURS

Melden bij betrokkene?

- Financiële onderneming ja/nee?
- Cryptografie voldoende bescherming
- Versleutelde persoonsgegevens
- Versleuteling adequaat
- Restrisico acceptabel
- Andere technische beschermingsmaatregelen
- Ongunstige gevolgen persoonlijke levenssfeer van de betrokkene
- Zwaarwegende redenen om de melding aan de betrokkene achterwege te laten

PELLICAAN
ADVOCATEN & ADVISEURS

Verschillen onder de AVG

Eisen zijn strenger (boetes hoger; deze kunnen oplopen tot € 20 mio of 4% van de jaaromzet)

- Binnen 72 uur melden. Lukt dit niet? à verklaring geven voor vertraging
- Betrokkene moet worden geïnformeerd over de inbreuk (melding aan betrokkene niet nodig bij maatregelen die conform de AVG zijn getroffen)
- Onder alle omstandigheden moet een verwerkingsverantwoordelijke alle inbreuken documenteren (art. 33 AVG)

PELLICAAN
ADVOCATEN & ADVISEURS

Voorbeelden van datalekken

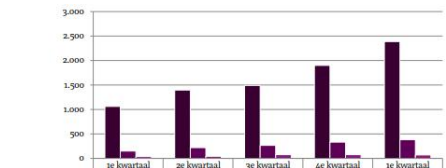
- Ransomware (WannaCry-cyberaanval)
- Werknemer veroorzaakt datalek (verlies van usb-stick maar ook een uitgeprinte klantenlijst)
- Gestolen laptops door inbraak
- Verkeerd verzenden van e-mail

PELLICAAN
ADVOCATEN & ADVISEURS

Overzicht AP feiten en cijfers 1e kwartaal 2017

Aantal meldingen	Type datalekken	Meest gelekte gegevens
2.317	45% persoonsgegevens aan verkeerde ontvanger	naam+ en adresgegevens, geboortedatum en BSN

Aantal meldingen in het eerste kwartaal van 2017



	1e kwartaal 2016	2e kwartaal 2016	3e kwartaal 2016	4e kwartaal 2016	1e kwartaal 2017
Nieuwe meldingen	1.061	1.396	1.491	1.901	2.388
Aanvullingen	150	220	267	333	382
Intrekkingen	36	43	76	77	71

Aanvullingen: Een datalekmelding kan later worden aangevuld als door onderzoek meer zicht is op de omvang of op de aard van de gegevens.
Intrekkingen: Een datalekmelding kan achteraf worden ingetrokken als na onderzoek blijkt dat het incident geen datalek was.

PELLICAAN
ADVOCATEN & ADVISEURS

Verwerkersovereenkomst

- Waar dient de verwerkersovereenkomst voor?
- Moet ik een verwerkersovereenkomst sluiten?
- Waar moet een verwerkersovereenkomst onder de AVG aan voldoen?
  - Kop en een staart
  - Algemene beschrijving van wat wordt overeengekomen
  - Instructies verwerken
  - Geheimhouding
  - Beveiliging
  - Subverwerkers
  - Privacyrechten
  - Pia (ander verplichtingen)
  - Verwijderen van gegevens
  - Aansprakelijkheden

PELLICAAN
ADVOCATEN & ADVISEURS

Privacy-proof zaken doen!

Doorgifte naar het buitenland

PELLICAAN
ADVOCATEN & ADVISEURS

Doorgifte naar het buitenland[1]

Doorgifte van persoonsgegevens naar een ander land is alleen toegestaan indien als dit land een passend beschermingsniveau heeft (en (onder de AVG) betrokkenen hun rechten kunnen afdwingen).

Binnen de EU (en Noorwegen, Liechtenstein en IJsland)
à toegestaan

Buiten de EU (en Noorwegen, Liechtenstein en IJsland)
à Alleen toegestaan in bepaalde gevallen

PELLICAAN
ADVOCATEN & ADVISEURS

Doorgifte naar het buitenland[2]

Doorgifte naar landen buiten de EU (en Noorwegen, Liechtenstein en IJsland):

- Passend beschermingsniveau (goedgekeurd door de Europese Commissie);
- Ondubbelzinnige toestemming van de betrokkene of een van de andere wettelijke uitzonderingen;
- Modelcontract goedgekeurd door de Europese Commissie;
- Vergunning (eigen of aangevuld contract);
- Bindende bedrijfsvoorschriften;
- Privacy Shield (voor doorgifte aan VS);
- Deelname aan goedgekeurde gedragscode (onder de AVG);
- Certificering (onder de AVG).

PELLICAAN
ADVOCATEN & ADVISEURS

Doorgifte naar het buitenland[3]

Privacy Shield

- Opvolger Safe Harbour-overeenkomst
- Vorm van certificering in de VS om tot passend beschermingsniveau te komen
- Controle en handhaving uitgesteld tot evaluatie Europese Commissie
- Vooralsnog toegestaan

Privacy Shield Framework

PELLICAAN
ADVOCATEN & ADVISEURS

Waarom aandacht voor privacy?

1. Reputatieschade voorkomen
2. Onderscheidend vermogen vergroten/acquisitie
3. Boetes voorkomen
4. Bescherming van data als asset
5. Risico's beperken bijv. bij financieringsaanvraag

PELLICAAN
ADVOCATEN & ADVISEURS

VRAGENRONDE

PELLICAAN
ADVOCATEN & ADVISEURS