General Data Protection Regulation

De belangrijkste gevolgen en verschillen ten opzichte van WBP

Versterking van klantrechten

- Klanten hebben meer te zeggen over hun data
- Transparante communicatie t.a.v. verwerking alvorens de data wordt verzameld
- Expliciete, opt-in toestemming voor marketing is vereist

Strengere verplichting

- Datalekken moeten binnen 72 uur worden gemeld aan de Autoriteit Persoonsgegevens
- Privacy by design en by default – moet in alle activiteiten, processen en beleid worden meegenomen

Duidelijke governance

- Verantwoordingsplicht: Aantoonbaar compliant zijn met de GDPR
- Verplichting tot het hebben van een Functionaris Gegevensbescherming (toezicht & advies)

Doorgifte data buiten EU

- Enkel indien adequate beveiliging kan worden gegarandeerd

Awareness

- Medewerkers moeten zich bewust zijn van de impact en de gevolgen van privacy

NVIA nederlandse vereniging inkomen adviseurs

AEGON

Wie is er al klaar voor?

Nieuws

23/02/2018 - Johan Rombouts

Veel organisaties nog niet klaar voor AVG

Ondanks dat 78% van de bestuurders van Nederlandse organisaties zich in toenemende mate zorgen maakt over de impact van de wetgeving AVG, is slechts 5% van mening dat zijn of haar organisatie over de juiste technische en procedurele vaardigheden beschikt. Dit is één van de belangrijkste conclusies uit de Global Forensic Data Analytics Survey van EY.

9 op de 10 bedrijven wereldwijd nog niet klaar voor AVG

Den Haag, 18 september 2017 – Een ruime meerderheid van de organisaties wereldwijd is nog niet goed voorbereid op de Algemene Verordening Gegevensbescherming (AVG). Dat blijkt uit een onderzoek onder ruim 1600 organisaties in opdracht van WatchGuard Technologies. Vooral buiten Europa leven misverstanden over de nieuwe Europese privacywetgeving, die internationaal bekendstaat als de General Data Protection Regulation.

Aanpak Aegon

2016: het been bijtrekken

Privacy Statement herzien, **Privacybeleid** voor medewerkers en klanten, **Bewerkersovereenkomsten** en **Datalekken**

2017: het krijgen van inzicht

Procesanalyse van **497** processen afgerond (Register van verwerkingen), **bewerkersovereenkomsten** en **Privacy Impact Assessments**

2018: verbeteren van privacy

Actieplannen voor issues, herzien **Privacy Statement** en **Privacybeleid** (Privacy by Design & Privacy by Default), verder implementeren **PIAs** voor producten, afronden implementeren **klantrechten** en **Awareness** campagne

(FG had Aegon al)

Waar te beginnen?

Sleutelwoord: verantwoording

Hulpmiddelen AP

- Stappenplan AVG van AP
- AVG-regelhulp (tip!) bedoeld voor Verwerkingsverantwoordelijken (= iedere organisatie die persoonsgegevens verwerkt en daarvoor zelf doel en middelen bepaalt)
- Consultatie AP (telefonisch, maar de AP geeft ook presentaties aan brancheorganisaties)

https://www.hulpbijprivacy.nl/

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg

https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/voorbereiding-op-de-avg

Het AVG-10 stappenplan

Met het AVG-10 stappenplan krijgt u snel overzicht op een aantal belangrijke AVG-thema's waar u zich op moet voorbereiden. Dit zijn:

1 Bewustwording
2 Rechten van betrokkenen
3 Overzicht verwerkingen
4 Data protection impact assessment (DPIA)
5 Privacy by design & privacy by default
6 Functionaris voor de gegevensbescherming
7 Meldplicht datalekken
8 Verwerkersovereenkomsten
9 Leidende toezichthouder
10 Toestemming

Verantwoording in de praktijk

- Startpunt: alle data in beeld krijgen
- Waarom?

  1 Op basis van de AVG mogen alleen die persoonsgegevens worden verwerkt die ook werkelijk nodig zijn en

  2 Waarvoor een wettelijke verwerkingsgrond bestaat

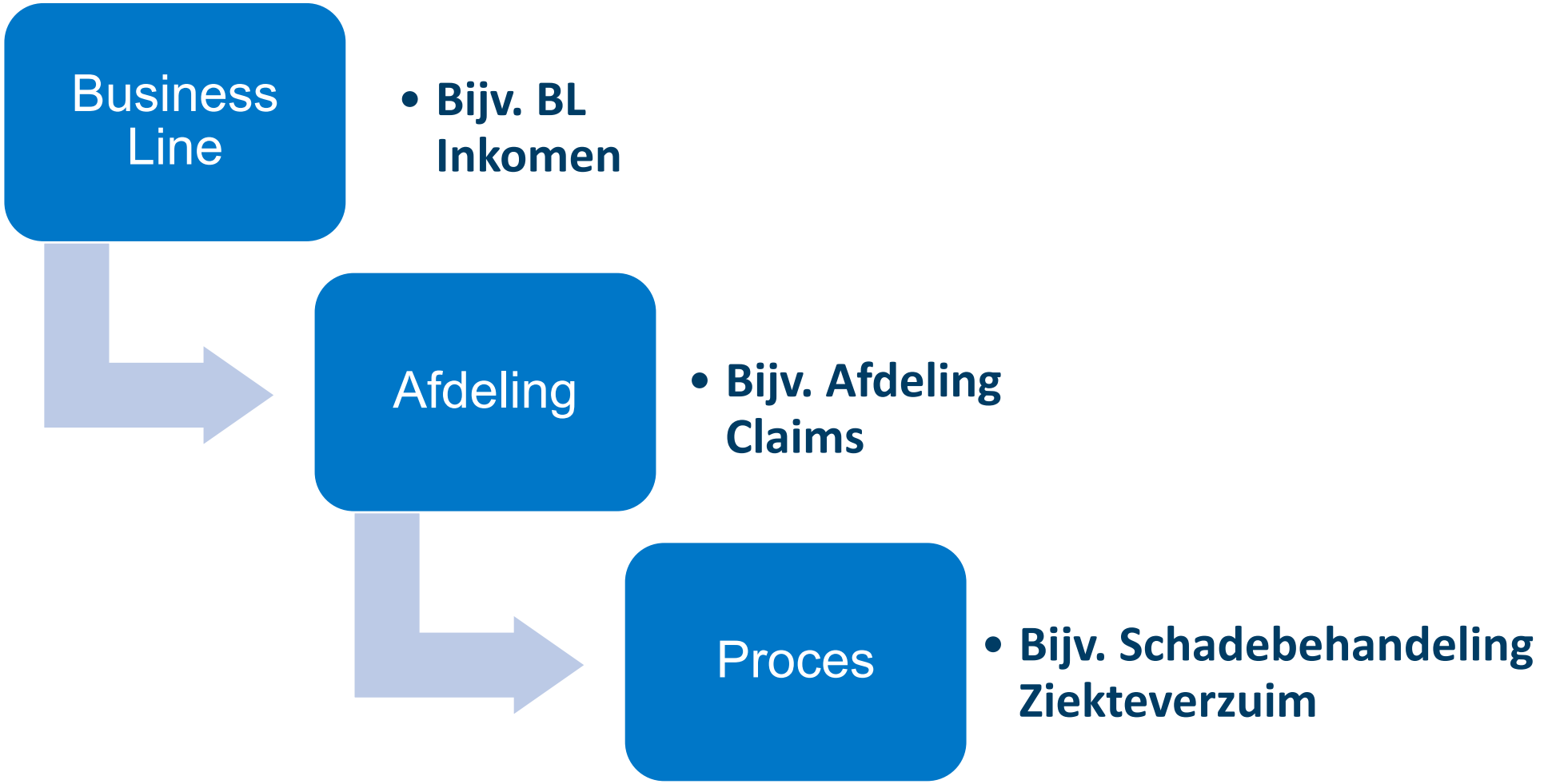
  3 Waarbij redelijke maatregelen zijn genomen om te voorkomen dat persoonsgegevens worden gebruikt of overgedragen voor doeleinden die niet zijn toegestaan (of worden gestolen)

Om dit te bereiken is een deugdelijke administratie rond persoonsgegevens nodig

- ✓ Tip: leg altijd een register van verwerkingen aan!
- ✓ Tip: maak het klein!

Inventariseren

Hoe heeft Aegon alle data in beeld gebracht?



Inventariseren

‘Gewone’ & bijzondere persoonsgegevens

Category of persons involved (Data Subjects)

- Customers, (web) visitors and leads
- Employees & job applicants
- Supplier/business partner
- Website and platform visitors
- Other (e.g. visitors)

Category personal data (Data Elements)

- Name
- Address
- House number
- Postal code
- City
- Phone number
- E-mail address
- License plate number
- Policy number
- Aegon identification number
- Bank account / credit card number
- Date of birth / age
- ID (e.g. passport) number
- Gender

- (Profile) picture
- Religion / philosophical beliefs
- Racial or ethnic origin
- Political affiliation
- Health data (physical/mental)
- Sexual preference / life
- Union membership
- (Alleged) Criminal past
- Social security number
- Login credentials
- IP address
- Internet surfing behaviour
- Genetic or biometric data
- Copy passport or ID card
- Location data
- Financial information

Legitimeren
Doel vaststellen

Data processing purposes

- Execution of an agreement
- Relationship management & contact
- Product- and business development, service improvement
- Marketing & customer/process analytics
- Safety / security
- Fight against fraud and Integrity within the financial sector
- Statistical and scientific purposes
- Provision of online services
- Legal/regulatory and other obligations

Customers

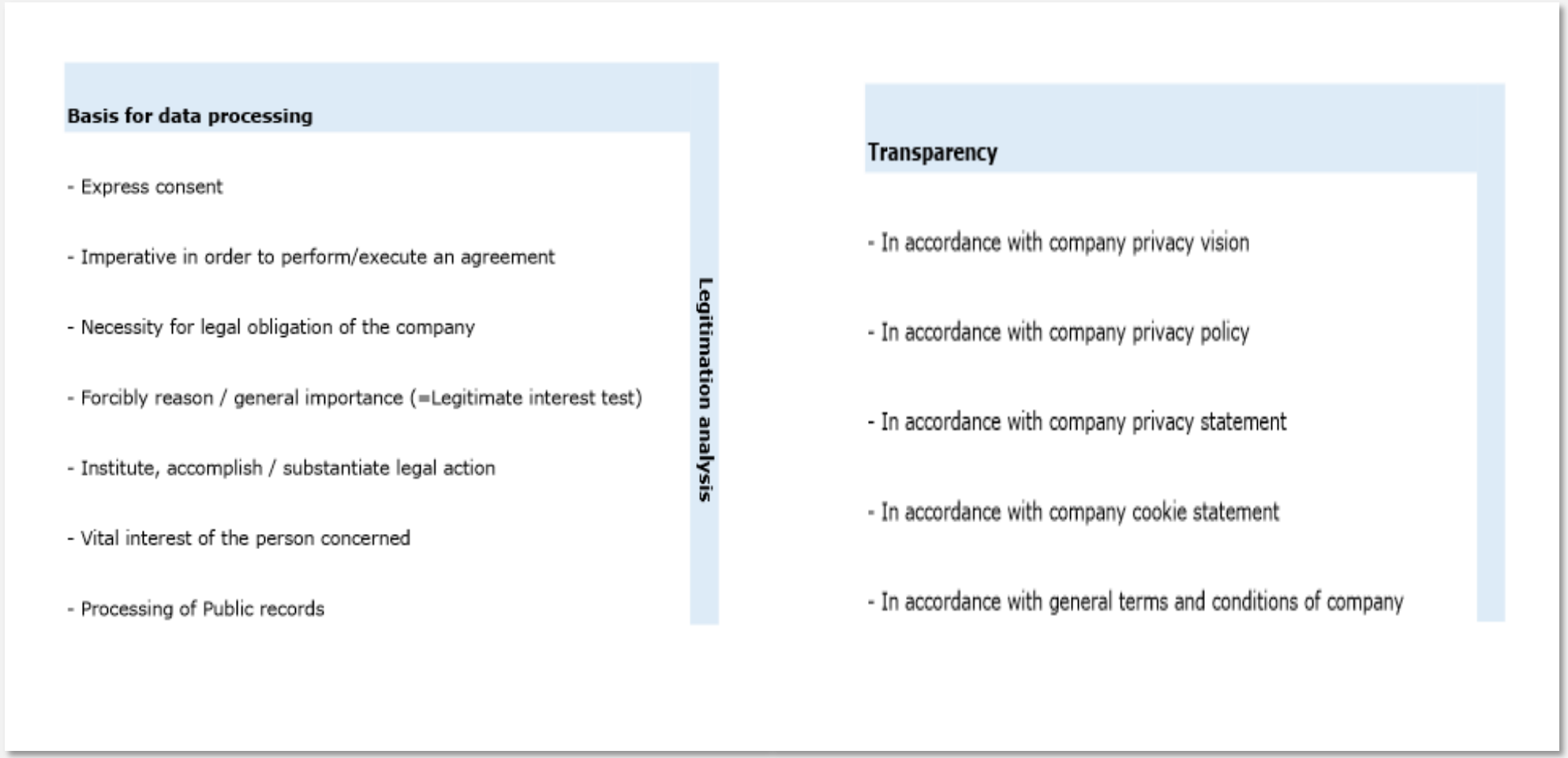
Data processing purposes

- Execution of an agreement
- General policy and internal management
- Evaluation of organisational and corporate structure / culture
- Health
- Fight against fraud and Integrity within the financial sector
- Legal/regulatory and other obligations
- Protection of vital concern of employees
- Representative advisory board
- (Former)Staff association

Employees

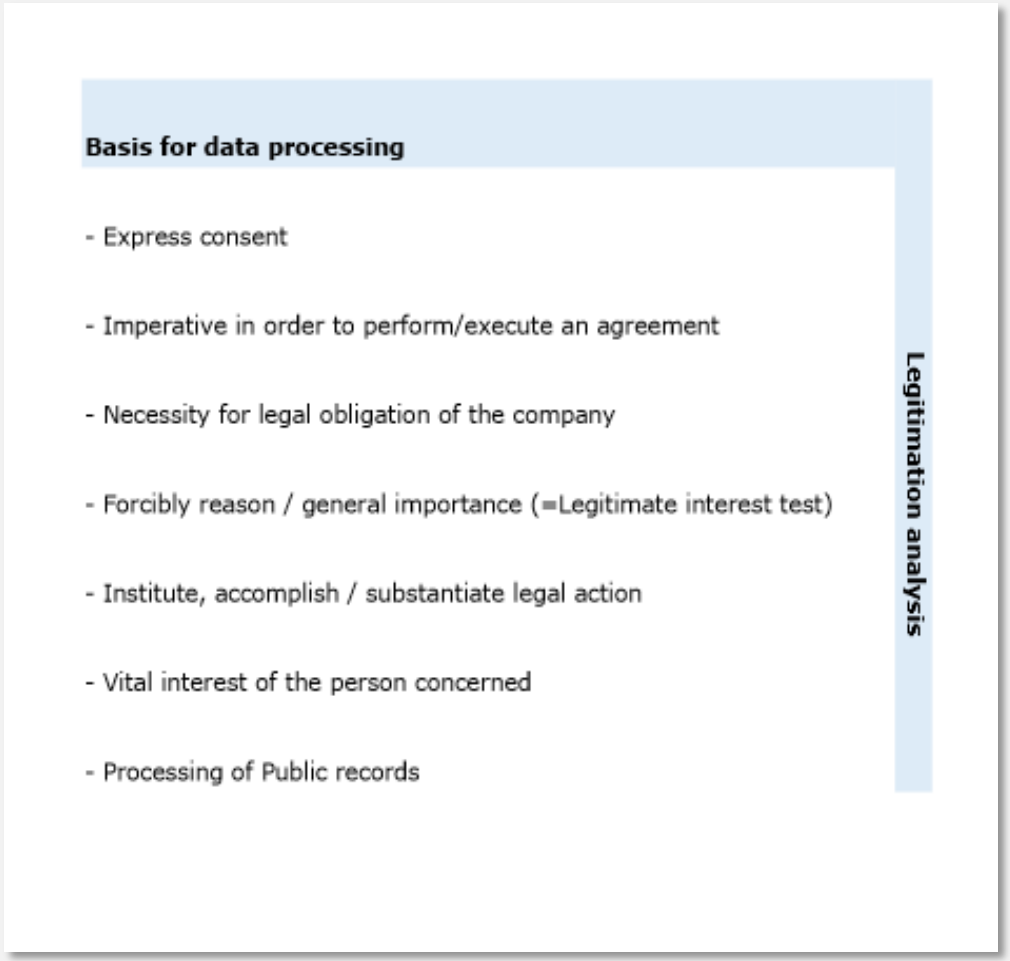
Legitimeren

Grondslag vaststellen



Legitimeren

Grondslag vaststellen



Wat betekent noodzakelijk?

1 grondslag is voldoende

Blijf weg van uitdrukkelijke toestemming!

Een paar vuistregels

- Als je de gegevens niet nodig hebt, verzamel ze dan niet
- Nodig = het doel kan zonder de gegevens niet worden bereikt
- Stel vast of er ook een grondslag tot verwerking bestaat
- Zorg dat de gegevens goed worden beschermd (let op bijv. dubbele authenticatie, afschermen van gegevens, e-mailverzending, etc.)
- De gegevens moeten accuraat en compleet zijn en worden onderhouden (let op datakwaliteit)
- Gebruik de gegevens niet voor andere doelen (geen verdere verwerkingen)
- Uitdrukkelijke toestemming moet aantoonbaar zijn (geen opt-out!)

Met wie worden de gegevens gedeeld?

Intern & Extern

Recipients of the Data	
Internal recipients	
Officers/directors	
HR manager, HR administration staff	
IT administrators / application developers	
facility management staff	
KNAB	Aegon NL labels
Cappital	
Kroodle	
EyeOpen	
Optas	
Other	
Nedasco	Other Aegon Group Companies
UMG	
AAM	
Other	

External Recipients	
Tax Authorities	Government
Ownership record keepers (Kadaster)	
Supervisors	
Central Government agency	
Local Government	
Public accountant	
Vendors	
Intermediaries	
Reinsurers	
Is data transferred to another country?	
If so to which country?	

Let op:

- **De wijze van delen: gebeurt dit veilig?**
- **Is er een overeenkomst nodig?**
- **Is voor de betrokkenen duidelijk dat de gegevens worden gedeeld?**

Andere aandachtspunten

- Hoe lang worden de gegevens bewaard?
- Waar worden de gegevens bewaard? (denk ook aan netwerkschijven en mailboxen)
- Worden er gegevens van minderjarigen verwerkt?
- Bij wettelijke verplichting: leg vast welke
- Zorg dat het privacy beleid, -statement en alg. voorwaarden een AVG update krijgen
- Maak een privacy notice (specifieke info voor de betrokkene(n) m.b.t. toegang, gebruik, en bescherming van gegevens)
- Denk na over beleid voor het geval als er echt iets misgaat! Wat biedt je de betrokkene?
- Bij IT testwerkzaamheden: zorg voor geanonimiseerde of gepseudonimiseerde testgegevens
- Zorg voor beleid op het gebied van datalekken

Hoe verder?

Analyseer de uitkomsten

- Waar ontbreken grondslagen?
- Waar bestaan overige issues?
- Waaruit bestaan die issues? (wat is er mis)

Risico inschatting en/of DPIA → **Aanpassingen**

Mogelijke issues & oplossingen

- **Er worden meer gegevens verwerkt dan nodig**
  (vb namen en BSN's van deelnemers in offertetraject)
- **Er zijn meer gegevens zichtbaar dan nodig**
  (vb BSN is op teveel plekken zichtbaar)
- **Er worden gegevens verwerkt zonder dat daartoe een grondslag bestaat**
  (vb diagnoses in niet-medisch dossier)
- **Bewaartermijnen zijn niet ingericht**

- **Er worden gegevens voor een ander doel gebruikt dan waarvoor ze zijn bedoeld**
  (vb direct marketing activiteiten aan de hand van gegevens van deelnemers, zonder dat daartoe toestemming is gevraagd)

- **'Overbodige' gegevens verwijderen**
  (I.c. deelnemer bestanden zonder naam en BSN insturen)
- **'deurtjes' inbouwen, 'afsterren', afschermen**

- **Dergelijke gegevens verwijderen. Let ook op vrije invoervelden!**

- **Leg per dossier vast wanneer de gegevens in beginsel moeten worden verwijderd**
- **Let op doelmatigheid! Verdere verwerkingen zijn niet toegestaan. Indien toch: vraag toestemming en leg dat vast**

Help een datalek!

- Sinds 1-1 2016 Wet Meldplicht Datalekken → lek moet binnen 72 uur gemeld worden aan de AP

- Datalek= een beveiligingsincident waarbij persoonsgegevens verloren zijn gegaan, gedeeld en/of toegankelijk zijn (geweest) voor onbevoegden, zonder reden gewijzigd zijn en/of onrechtmatig verwerkt zijn

- Kan van alles zijn: verzenden van stukken naar een onjuist e-mailadres, gegevens van een ander zichtbaar in een portal, een gestolen apparaat, een inbreuk door een hack, Maar ook: stukken op de printer, etc.

- Een datalek is altijd een beveiligingsincident, maar niet ieder beveiligingsincident is een datalek

Een paar internationale feiten

- IBM onderzoekt jaarlijks alle datalekken wereldwijd
- 419 bedrijven in 13 landen onderzocht (2017; NL zat hier niet bij)
- Meeste datalekken ontstaan ten gevolge van hacking (47%)
- Menselijke fouten (28%) en systeem fouten (25%) staan op plaats 2 en 3
- Alle onderzochte organisaties hadden datalekken waarbij tussen de 2.600 en 100.000 bestanden/gegevens zijn gelekt
- De gemiddelde totale kosten bedroegen $3,62 miljoen
- Per datalek was dit: $141,-

Het complete onderzoeksrapport is te downloaden via https://www.ibm.com/security/data-breach/

Impact beperken

Impact van datalekken te beperken door:

- Overbodige gevoelige persoonsgegevens van documenten verwijderen (zowel fysiek als digitaal)
- Goede beveiliging van systemen en applicaties
- 4 ogen controles op gevoelige processen
- Zorg voor bewustwording bij werknemers

Autoriteit Persoonsgegevens lekte per ongeluk namen van personeel

Gepubliceerd: 16 maart 2018 10:19
Laatste update: 16 maart 2018 11:12

De Autoriteit Persoonsgegevens, waarbij bedrijven datalekken verplicht moeten melden, heeft zelf per ongeluk de namen van werknemers openbaar gemaakt.

Organisatorisch:

- Richt een incidenten beleid in
- Leg ook hier een register of database aan
- Maak actieplannen om nieuwe gevallen te voorkomen

Gegevens 50 miljoen kiezers VS via Facebook buitgemaakt

ZATERDAG, 19:40 AANGEPAST GISTEREN, 07:55 BUITENLAND

De gegevens van 50 miljoen vooral Amerikaanse Facebookprofielen zijn op geraffineerde wijze buitgemaakt door het bedrijf Cambridge Analytica, dat destijds werd geleid door Steve Bannon, die later een sleutelrol speelde in de campagne van Donald Trump.

Voordelen AVG

- ✓ Kans om interne processen te verbeteren
- ✓ En daarmee de organisatie succesvoller te maken
- ✓ Kans om te innoveren en technologie in te zetten om veiliger en productiever te werken
- ✓ Bij dataminimalisatie en bij verwerken van minder gevoelige gegevens wordt het beveiligen van gegevens minder complex
- ✓ Minder gegevens → minder capaciteit van opslagservers nodig → voordeliger
- ✓ Maar de allerbelangrijkste: een goede naleving van de AVG schept vertrouwen!

Vragen??

KEEP
CALM
AND
COMPLY WITH
GDPR

Dank je!

Aegonplein 50, 2591 TV
Den Haag
Telefoon: 070 344 3210

Postbus 202
2501 CE Den Haag