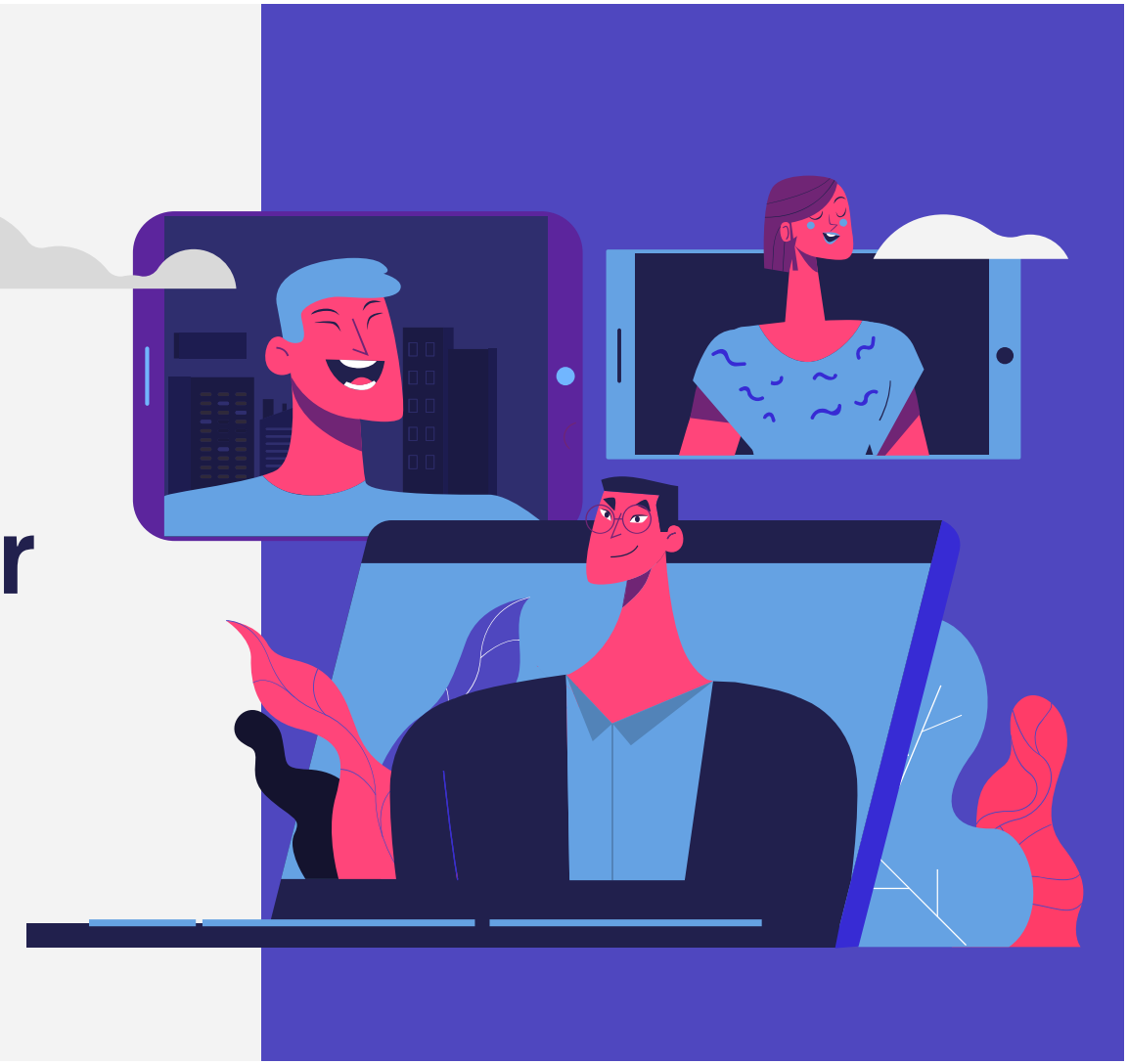
OOSTENDE
ECONOMISCH HUIS
ONDERNEEMT U MEE

Awareness GDPR & Cyber Security

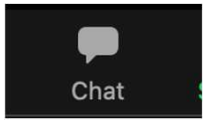


Lexit
lawyers and consultants at privacy law

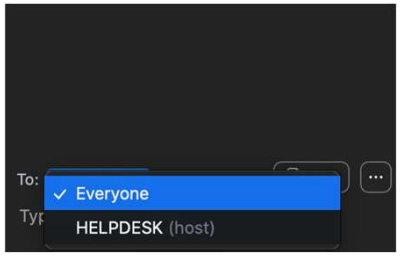
AGENTSCHAP INNOVEREN & ONDERNEMEN
Vlaanderen is ondernemen

Welkom bij de GDPR – Cyber security webinar van Economisch Huis Oostende

1. Jouw microfoon en webcam staan uit, dit om de webinar vlot te laten verlopen



2. Indien je problemen hebt kan je dit melden via de chatbutton



3. Klik hierna bij “aan/to” op Helpdesk, zo kan je een privégesprek starten met de helpdesk om eventuele problemen op te lossen.

4. Heb je vragen tijdens de webinar? Stel deze gerust in de algemene chat (EVERYONE), we verzamelen de vragen en beantwoorden deze achteraf.

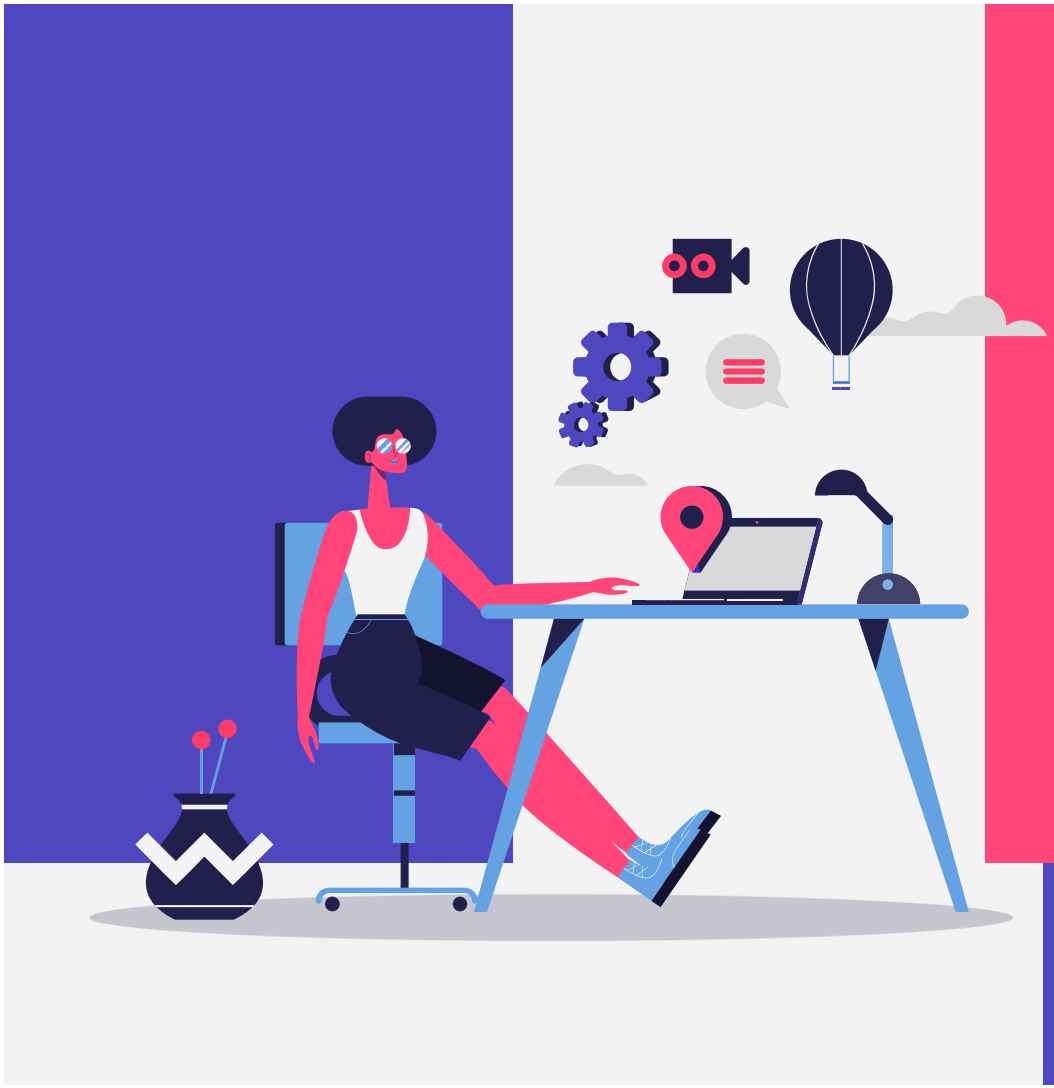
OOSTENDE
ECONOMISCH HUIS
OndernemtUMee

01 GDPR kort uitgelegd

02 Incidenten en datalekken

03 Hoe incidenten beperken?

04 Hackers @ Work

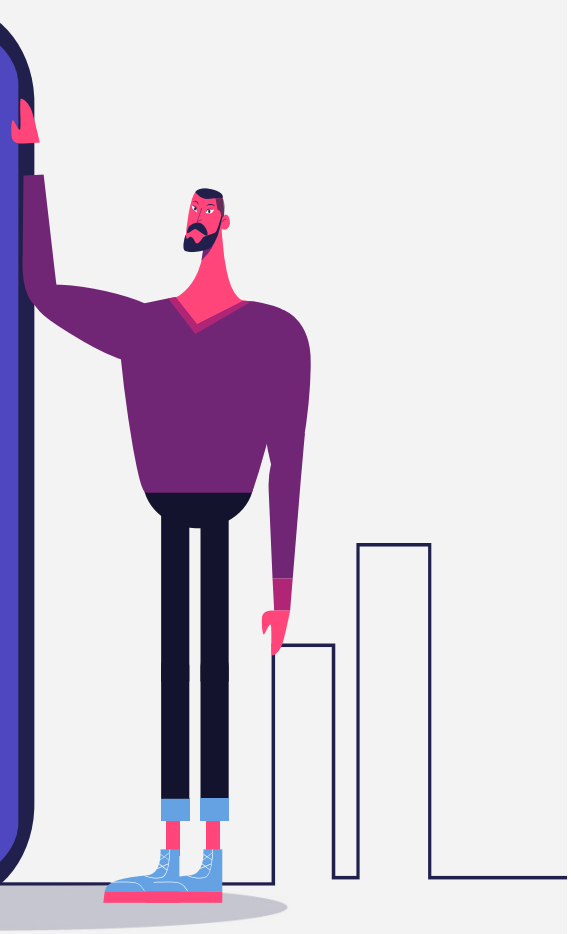


01 GDPR IN HET KORT(ST MOGELIJKE)

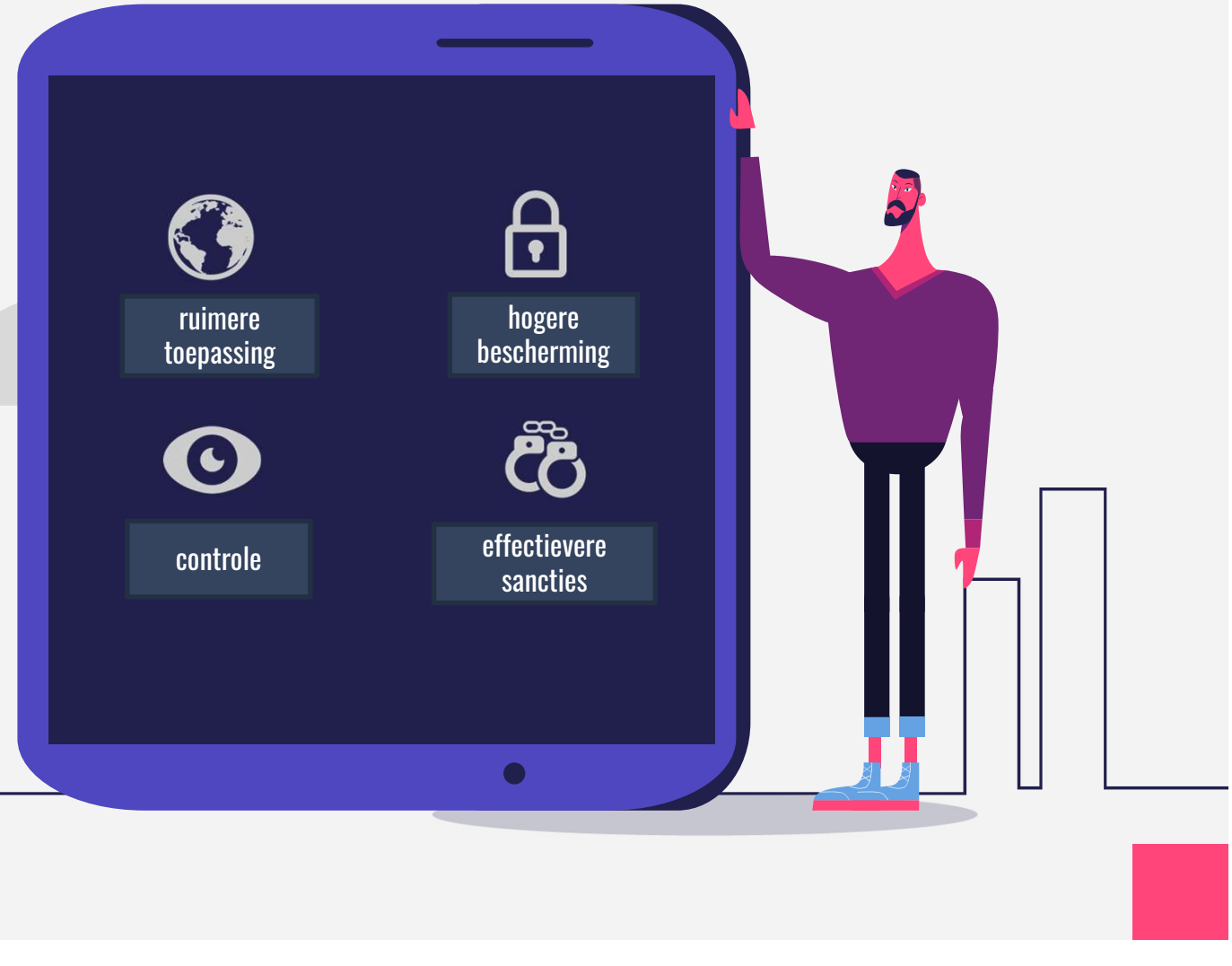
DOEL UITEENZETTING

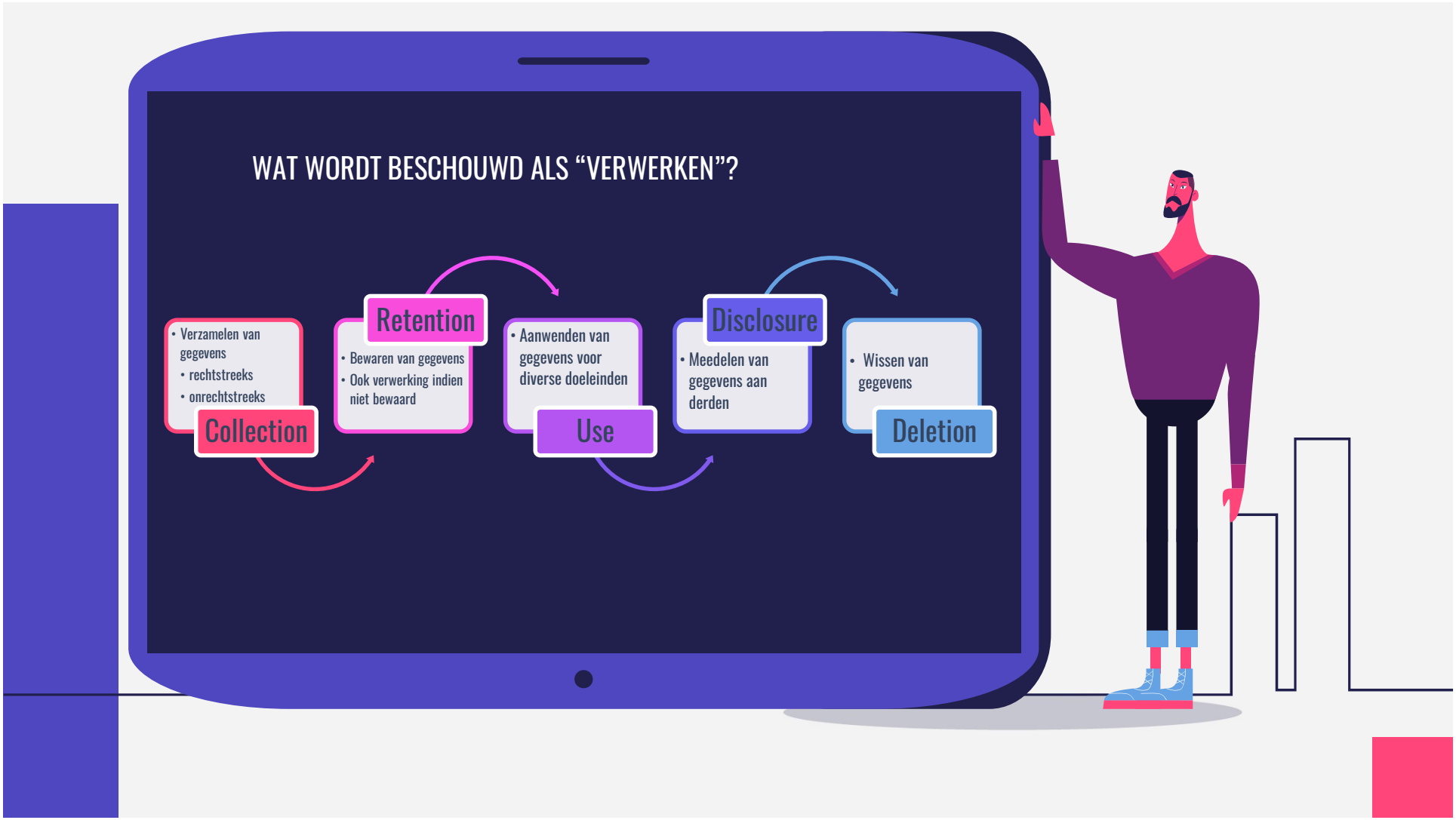
DOEL UITEENZETTING

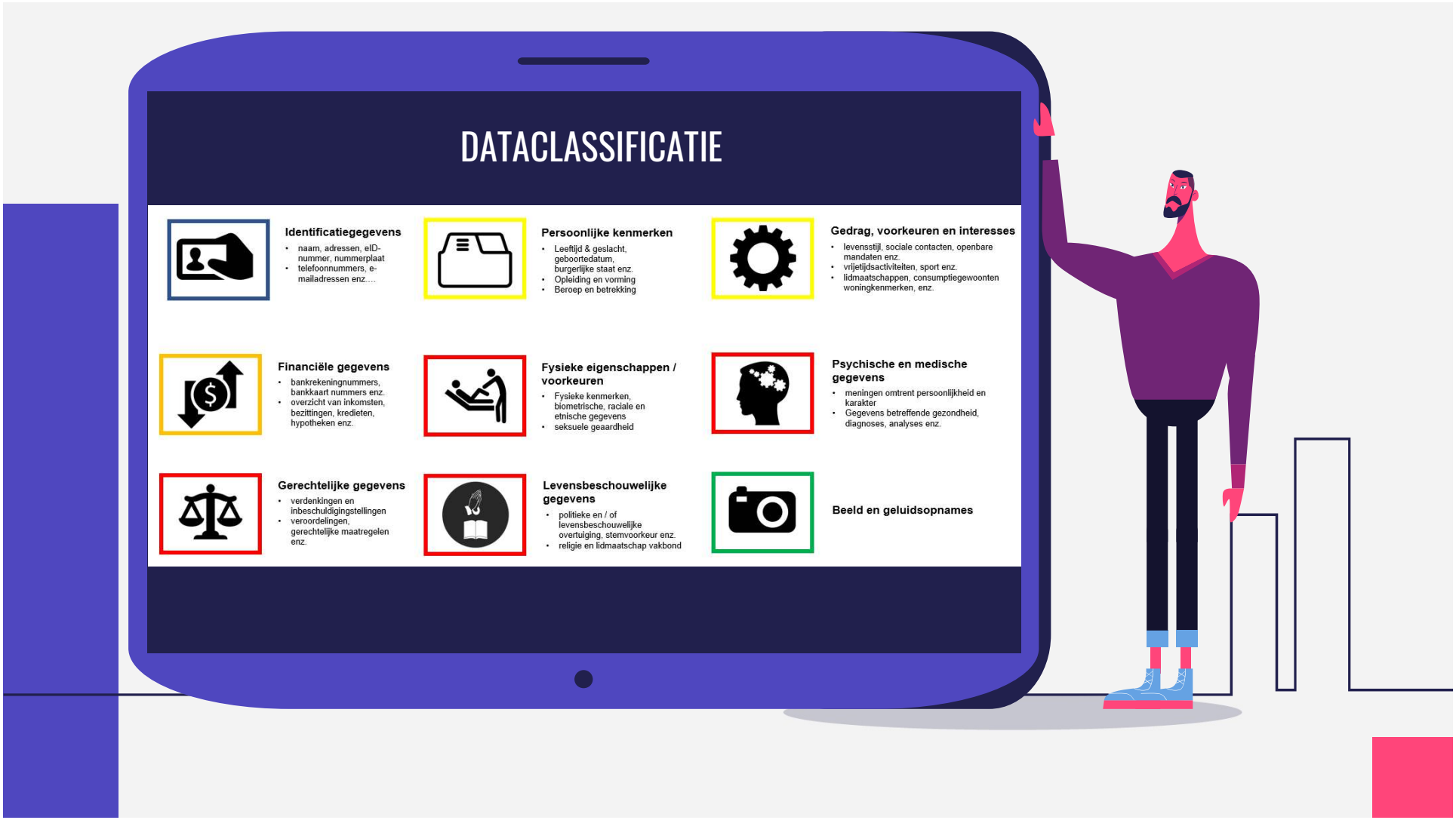
- Sterke basis over de begrippen
- Vat krijgen op waarover de GDPR nu werkelijk gaat
- De theorie van de GDPR toepassen in de praktijk
- Aan de hand van voorbeelden u toelaten een (eerste) GDPR-beoordeling te maken van privacy kwesties



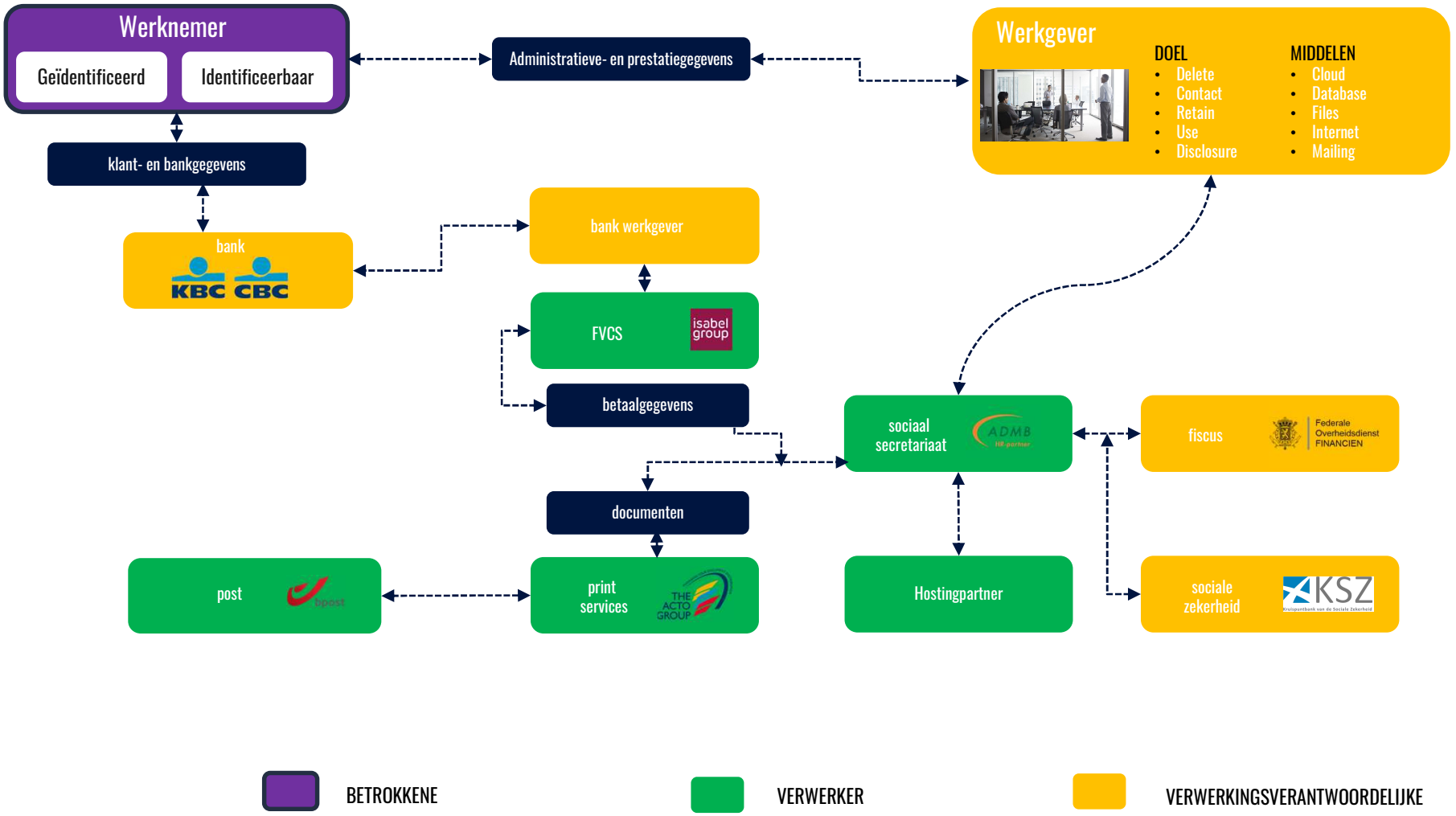
UPDATE PRIVACYWET 1992




WAT WORDT BESCHOUWD ALS “VERWERKEN”?
• Verzamelen van gegevens
• rechtstreeks
• onrechtstreeks
Collection
Retention
• Bewaren van gegevens
• Ook verwerking indien niet bewaard
• Aanwenden van gegevens voor diverse doeleinden
Use
Disclosure
• Meedelen van gegevens aan derden
• Wissen van gegevens
Deletion


DATACLASSIFICATIE
Identificatiegegevens
naam, adressen, eID-nummer, nummerplaat
telefoonnummers, e-mailadressen enz....
Persoonlijke kenmerken
Leeftijd & geslacht, geboortedatum, burgerlijke staat enz.
Opleiding en vorming
Beroep en betrekking
Gedrag, voorkeuren en interesses
levensstijl, sociale contacten, openbare mandaten enz.
vrijetijdsactiviteiten, sport enz.
lidmaatschappen, consumptiegewoonten woningkenmerken, enz.
Financiële gegevens
bankrekeningnummers, bankkaart nummers enz.
overzicht van inkomsten, bezittingen, kredieten, hypotheken enz.
Fysieke eigenschappen / voorkeuren
Fysieke kenmerken, biometrische, raciale en etnische gegevens
seksuele geaardheid
Psychische en medische gegevens
meningen omtrent persoonlijkheid en karakter
Gegevens betreffende gezondheid, diagnoses, analyses enz.
Gerechtelijke gegevens
verdenkingen en inbeschuldigingstellingen
veroordelingen, gerechtelijke maatregelen enz.
Levensbeschouwelijke gegevens
politieke en / of levensbeschouwelijke overtuiging, stemvoorkeur enz.
religie en lidmaatschap vakbond
Beeld en geluidsopnames

VERSCHILLENDE ROLLEN

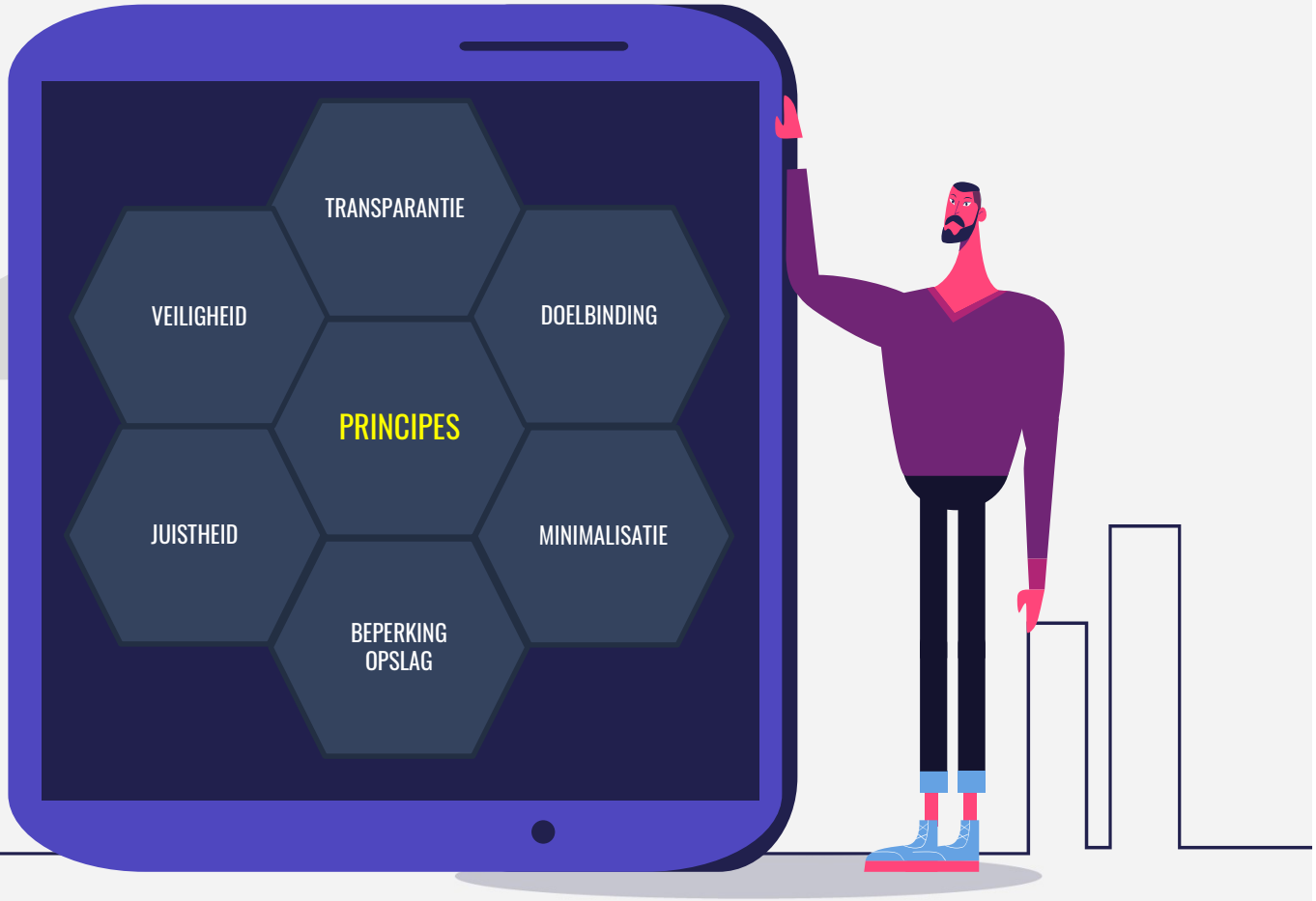

Werknemer
Geïdentificeerd
Identificeerbaar
Administratieve- en prestatiegegevens
Werkgever
DOEL
Delete
Contact
Retain
Use
Disclosure
MIDDELEN
Cloud
Database
Files
Internet
Mailing
klant- en bankgegevens
bank
KBC CBC
bank werkgever
FVCS
isabel group
betaalgegevens
sociaal secretariaat
ADMB HR-partner
fiscus
Federale Overheidsdienst FINANCIEN
documenten
post
bpost
print services
THE ACTO GROUP
Hostingpartner
sociale zekerheid
KSZ
BETROKKENE
VERWERKER
VERWERKINGSVERANTWOORDELIJKE

10 KERN-VERPLICHTINGEN

1. Verwerkingsgrond
2. Verwerkingsprincipes
3. Rechten van betrokkenen
4. TOM’s voor veilige verwerking
5. Data Breaches
6. DPO
7. Verwerkingsregister
8. Contracten met verwerkers
9. Privacy by design / default
10. DPIA

1. GRONDSLAGEN VOOR HET VERWERKEN VAN PERSOONS-GEGEVENS

2. PRINCIPES BIJ HET VERWERKEN VAN PERSOONS-GEGEVENS



- Recht op transparantie
- Recht op inzage
- Recht op overdraagbaarheid van gegevens (= nieuw)
- Recht op rectificatie
- Recht op beperking van verwerking
- Recht op weigering geautomatiseerde beslissing (profiling)
- Recht op gegevenswissing (vergeet me)
- Recht op bezwaar

3. RECHTEN VAN BETROKKENEN?

MAATREGELEN (TOM'S)

administratieve = vnl. documenteren

organisatorische = *business processen*

technische = fysieke (plaats) en netwerk-technische bescherming

4. TECHNISCH-ORGANISATORISCHE MAATREGELEN

MELDING AAN DE GBA

Wanneer er een datalek is

- VV: binnen de 72u
- V: zonder onredelijke vertraging

MELDING AAN DE BETROKKENEN

Wanneer er een datalek is + wanneer er een hoog risico op aantasting van diens rechten is

Opm.: GBA = Gegevensbeschermingsautoriteit

5. DATA BREACHES (datalekken)

DUBBELE MELDINGSPLICHT

Taak:

Adviseren / informeren / toezicht en samenwerken

Verplicht?

JA, o.a. bij overheidsinstellingen

Skills:

Bijzondere deskundigheid

6. DPO

Inhoud register (voor DC)

- Identiteit & contactgegevens verwerkingsverantwoorde-lijke
- Doelstellingen van de verwerking
- (categorieën van) Verwerkte persoonlijke data & betrokkenen
- Overdracht buiten de EU
- TOM's & Retention & deletion policy
- Verwerkingsgronden

7. REGISTER VAN VERWERKINGS-ACTIVITEITEN

- Enkel contracteren met adequate verwerkers! (controle- en verificatieplicht!)
- Verwerken op basis van schriftelijke instructies
- Vertrouwelijkheids-verplichtingen
- Technische maatregelen ter beveiliging
- Instructies rond Subverwerkers

8. VERWERKERS-CONTRACTEN

By design

- Aandacht besteden aan privacy verhogende maatregelen bij ontwikkeling nieuwe diensten en systemen

By default

- privacy is de standaard instelling van een programma, app, website, dienst of apparaat.

9. PRIVACY BY DESIGN - DEFAULT

Data Protection Impact Assessment

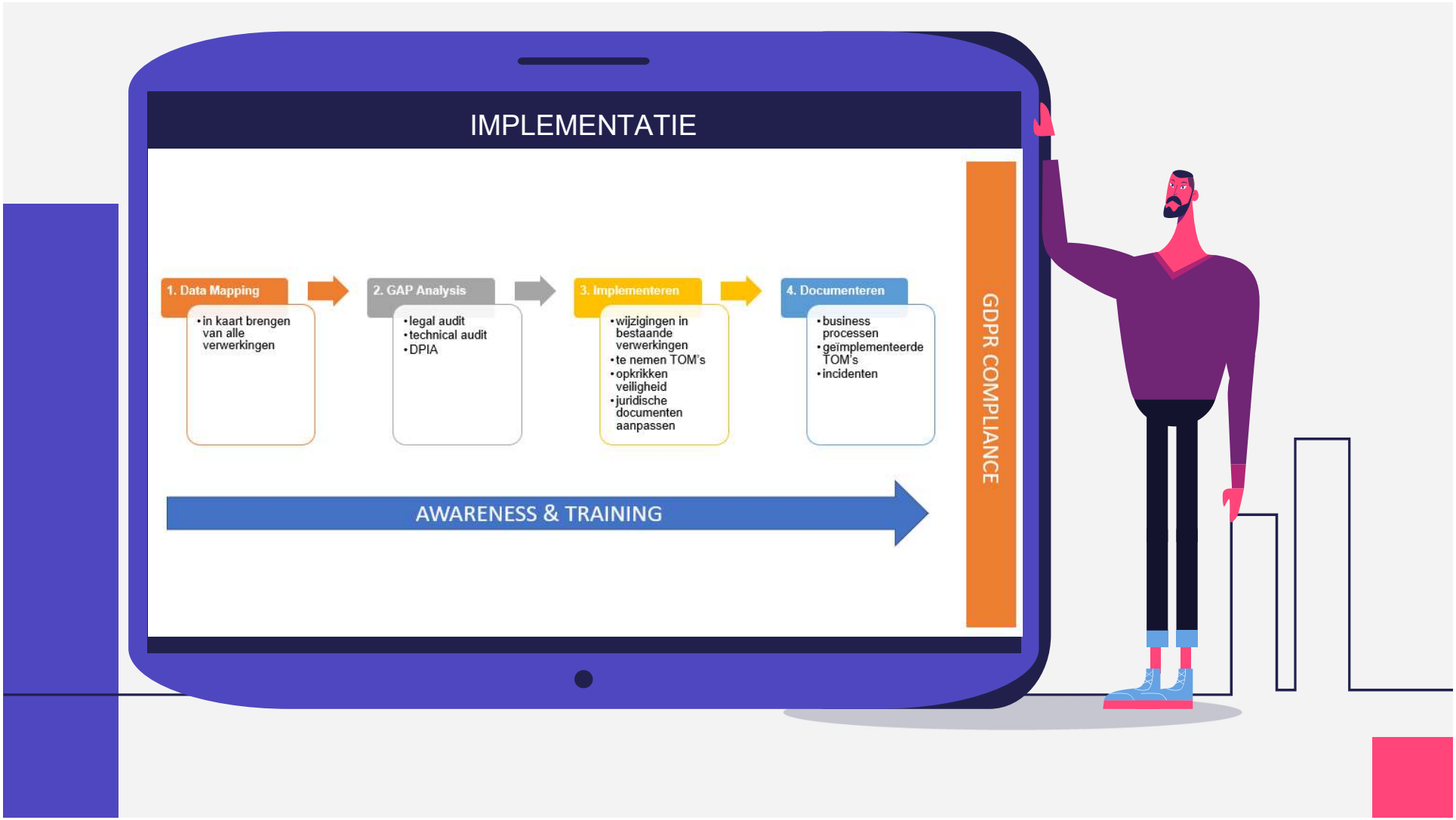
- risico analyse
- vóór aanvang verwerking

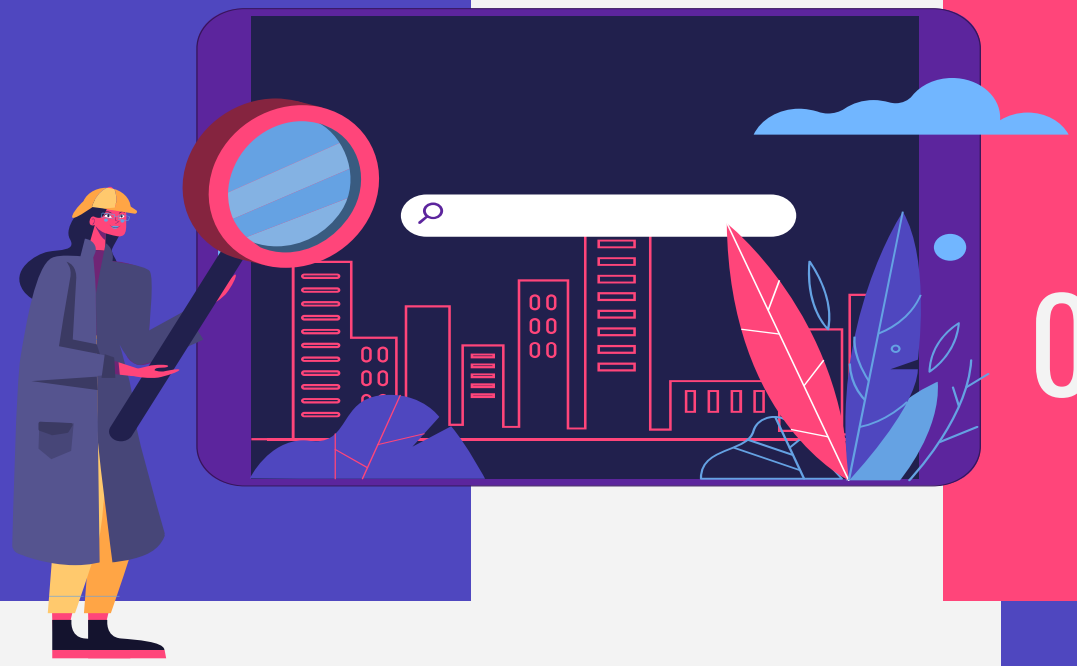
Doel: bij aanvang nieuwe verwerking garanties voor privacy in proces inbakken

Wanneer?

- nieuwe technologieën
- hoog risico

10. DPIA


IMPLEMENTATIE
1. Data Mapping
• in kaart brengen van alle verwerkingen
2. GAP Analysis
• legal audit
• technical audit
• DPIA
3. Implementeren
• wijzigingen in bestaande verwerkingen
• te nemen TOM's
• opkrikken veiligheid
• juridische documenten aanpassen
4. Documenteren
• business processen
• geïmplementeerde TOM's
• incidenten
AWARENESS & TRAINING
GDPR COMPLIANCE



02 INCIDENTEN EN DATALEKKEN

VERSCHIL INCIDENT – DATALEK?

WAT IS EEN **BEVEILIGINGSINCIDENT**?

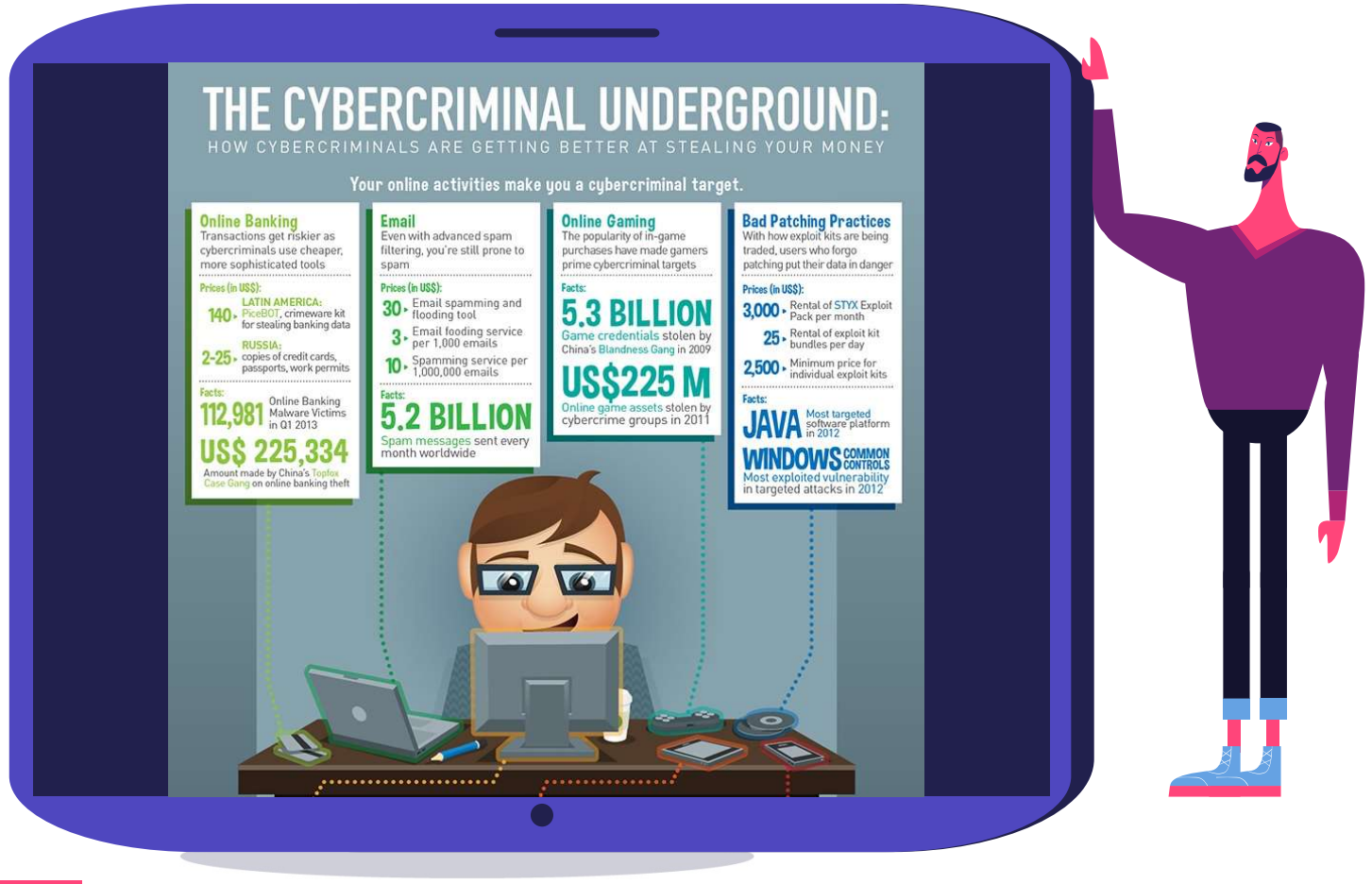
= gebeurtenis waarbij de **mogelijkheid** bestaat dat de **vertrouwelijkheid**, **integriteit** of **beschikbaarheid** van informatie of informatie verwerkende systemen **in gevaar is of kan komen**.

Niet elk beveiligingsincident is een datalek.

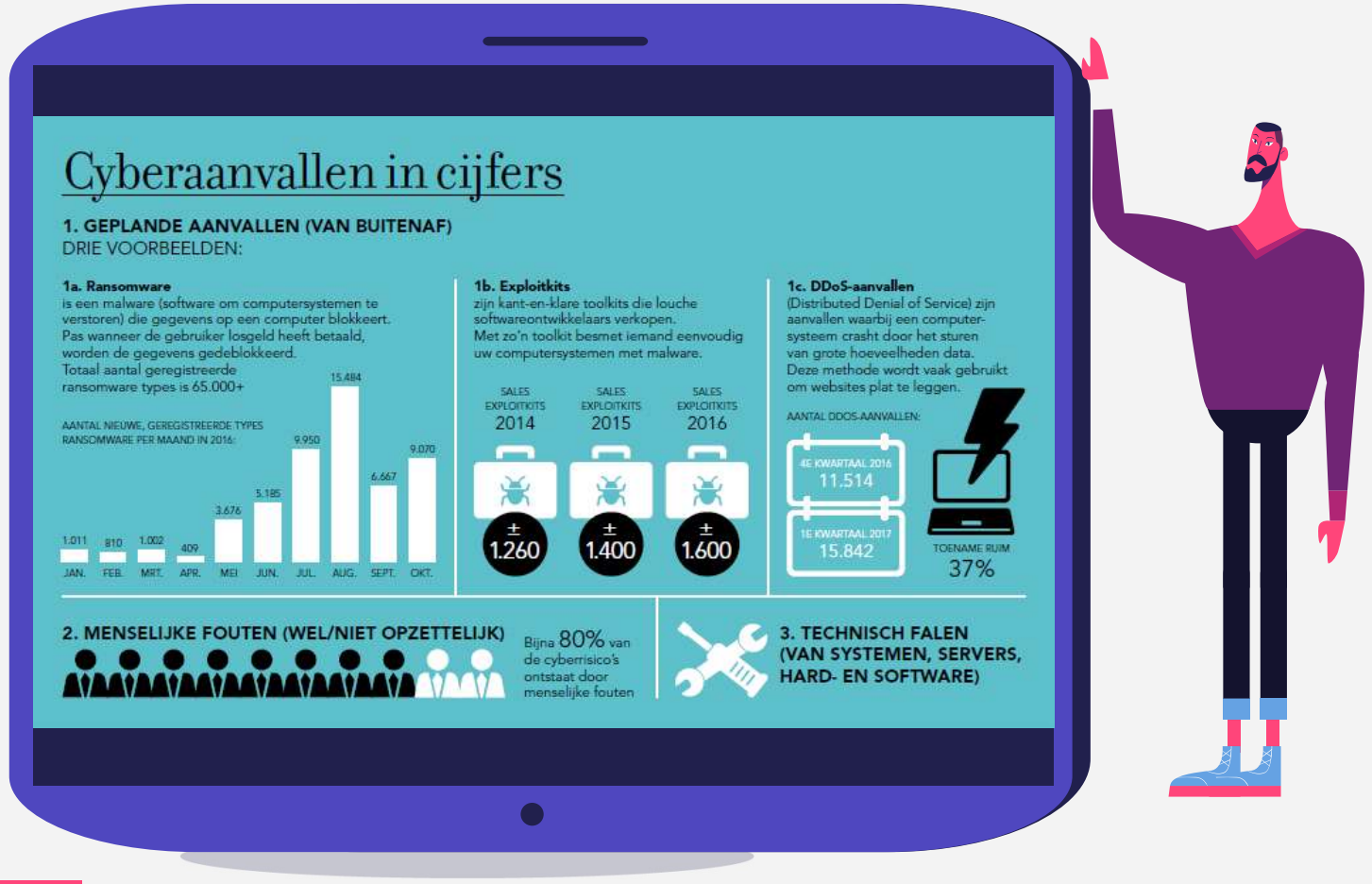
WAT IS EEN **DATALEK**?

= **beveiligingsincident** waarbij **persoonsgegevens** in handen van onbevoegden zijn gekomen, voor onbevoegden toegankelijk waren, of ‘zijn verloren’.

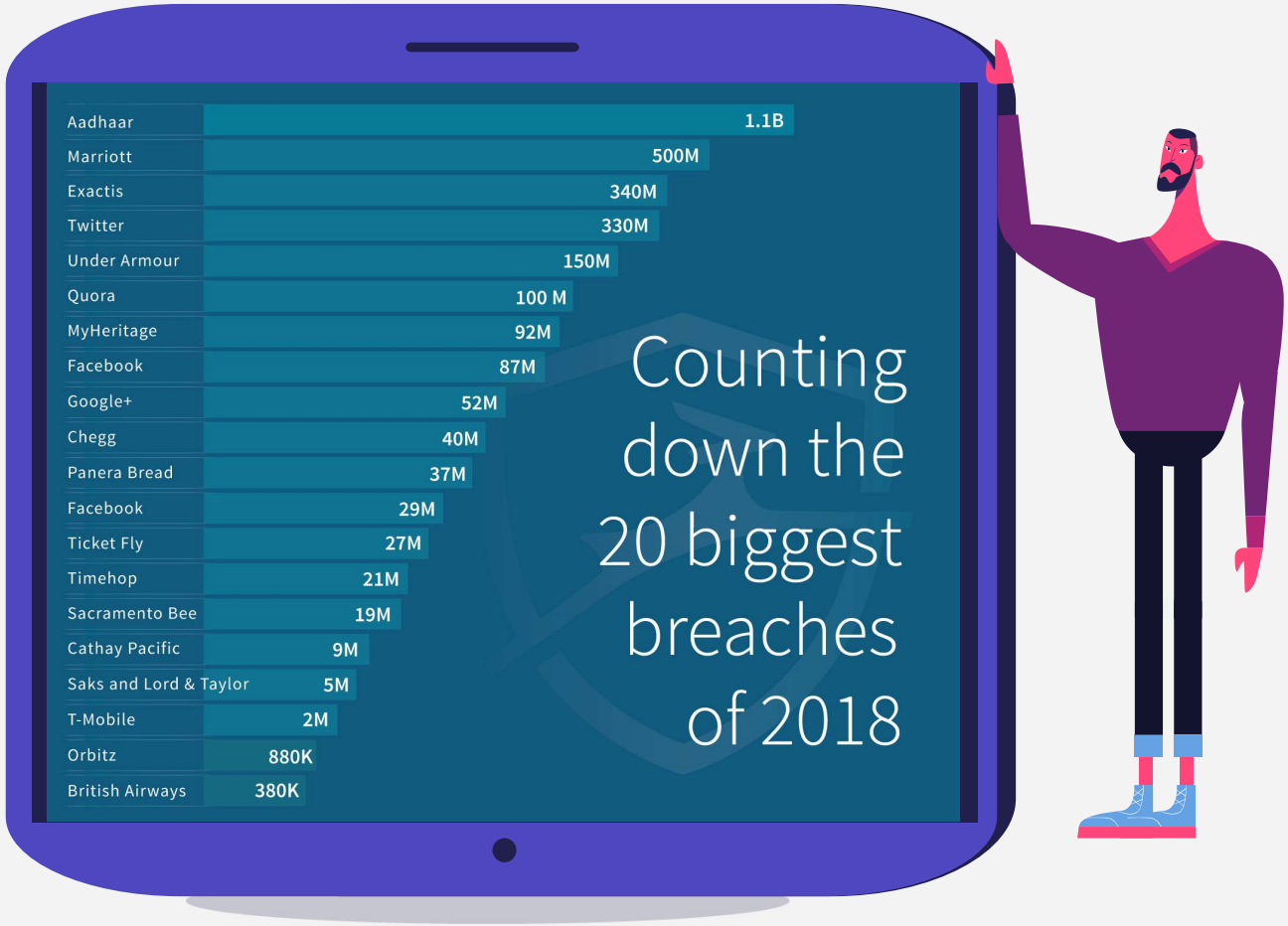
VOORBEELDEN VAN INCIDENTEN


THE CYBERCRIMINAL UNDERGROUND:
HOW CYBERCRIMINALS ARE GETTING BETTER AT STEALING YOUR MONEY
Your online activities make you a cybercriminal target.
Online Banking
Transactions get riskier as cybercriminals use cheaper, more sophisticated tools
Prices (in US$):
140 LATIN AMERICA: PiceBOT, crimeware kit for stealing banking data
2-25 RUSSIA: copies of credit cards, passports, work permits
Facts:
112,981 Online Banking Malware Victims in Q1 2013
US$ 225,334
Amount made by China's Topfox Case Gang on online banking theft
Email
Even with advanced spam filtering, you're still prone to spam
Prices (in US$):
30 Email spamming and flooding tool
3 Email fooding service per 1,000 emails
10 Spamming service per 1,000,000 emails
Facts:
5.2 BILLION
Spam messages sent every month worldwide
Online Gaming
The popularity of in-game purchases have made gamers prime cybercriminal targets
Facts:
5.3 BILLION
Game credentials stolen by China's Blandness Gang in 2009
US$225 M
Online game assets stolen by cybercrime groups in 2011
Bad Patching Practices
With how exploit kits are being traded, users who forgo patching put their data in danger
Prices (in US$):
3,000 Rental of STYX Exploit Pack per month
25 Rental of exploit kit bundles per day
2,500 Minimum price for individual exploit kits
Facts:
JAVA Most targeted software platform in 2012
WINDOWS COMMON CONTROLS
Most exploited vulnerability in targeted attacks in 2012

CIJFERS


Cyberaanvallen in cijfers
1. GEPLANDE AANVALLEN (VAN BUITENAF)
DRIE VOORBEELDEN:
1a. Ransomware
is een malware (software om computersystemen te verstoren) die gegevens op een computer blokkeert. Pas wanneer de gebruiker losgeld heeft betaald, worden de gegevens gedeblokkeerd.
Totaal aantal geregistreerde ransomware types is 65.000+
AANTAL NIEUWE, GEREGISTREERDE TYPES RANSOMWARE PER MAAND IN 2016:
1.011
810
1.002
409
3.676
5.185
9.950
15.484
6.667
9.070
JAN.
FEB.
MRT.
APR.
MEI
JUN.
JUL.
AUG.
SEPT.
OKT.
1b. Exploitkits
zijn kant-en-klare toolkits die louche softwareontwikkelaars verkopen.
Met zo'n toolkit besmet iemand eenvoudig uw computersystemen met malware.
SALES EXPLOITKITS 2014
SALES EXPLOITKITS 2015
SALES EXPLOITKITS 2016
± 1.260
± 1.400
± 1.600
1c. DDoS-aanvallen
(Distributed Denial of Service) zijn aanvallen waarbij een computer-systeem crasht door het sturen van grote hoeveelheden data.
Deze methode wordt vaak gebruikt om websites plat te leggen.
AANTAL DDOS-AANVALLEN:
4E KWARTAAL 2016
11.514
1E KWARTAAL 2017
15.842
TOENAME RUIM
37%
2. MENSELIJKE FOUTEN (WEL/NIET OPZETTELIJK)
Bijna 80% van de cyberrisico's ontstaat door menselijke fouten
3. TECHNISCH FALEN (VAN SYSTEMEN, SERVERS, HARD- EN SOFTWARE)

CIJFERS

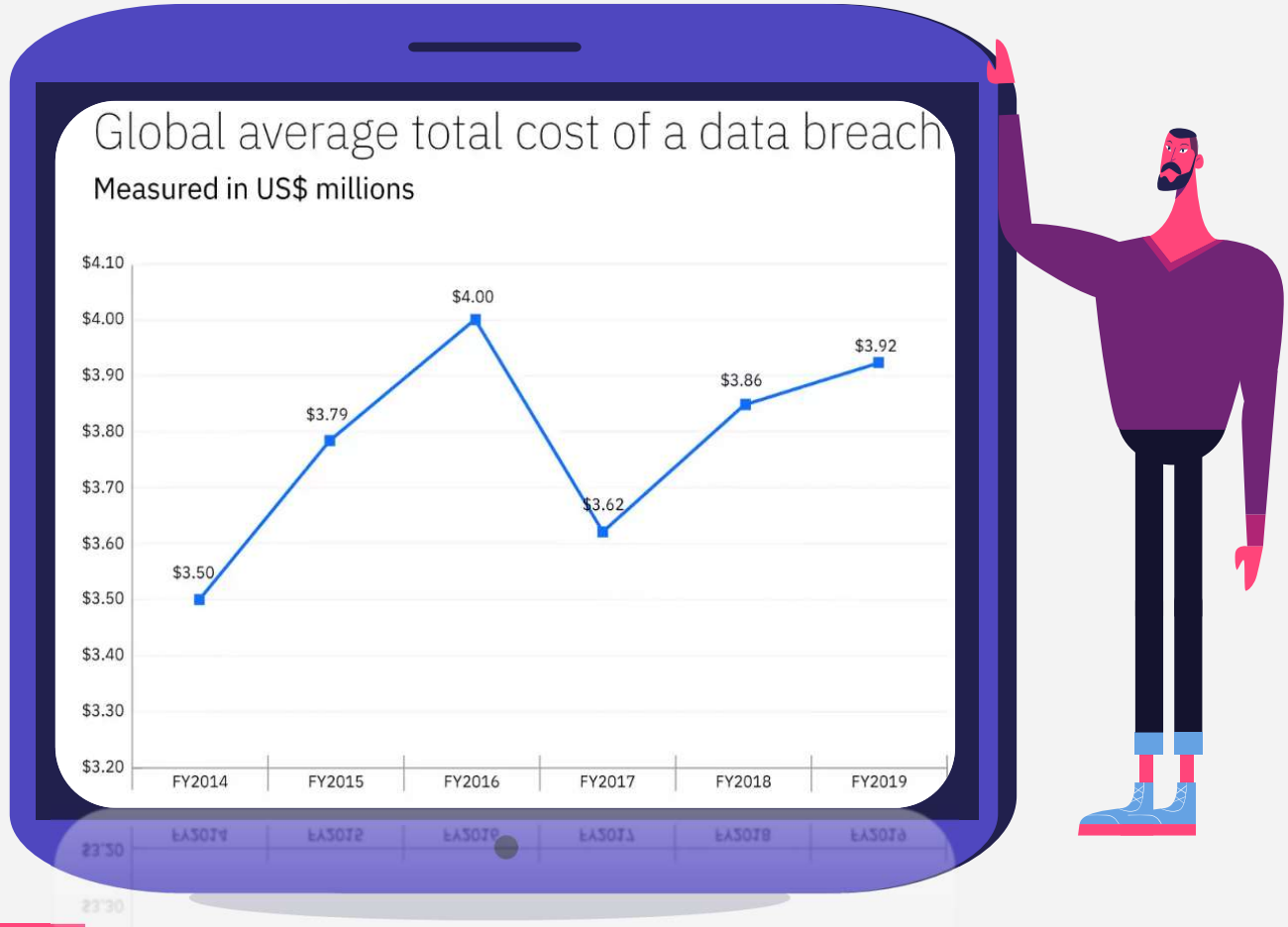

Aadhaar 1.1B
Marriott 500M
Exactis 340M
Twitter 330M
Under Armour 150M
Quora 100 M
MyHeritage 92M
Facebook 87M
Google+ 52M
Chegg 40M
Panera Bread 37M
Facebook 29M
Ticket Fly 27M
Timehop 21M
Sacramento Bee 19M
Cathay Pacific 9M
Saks and Lord & Taylor 5M
T-Mobile 2M
Orbitz 880K
British Airways 380K
Counting down the 20 biggest breaches of 2018

CIJFERS

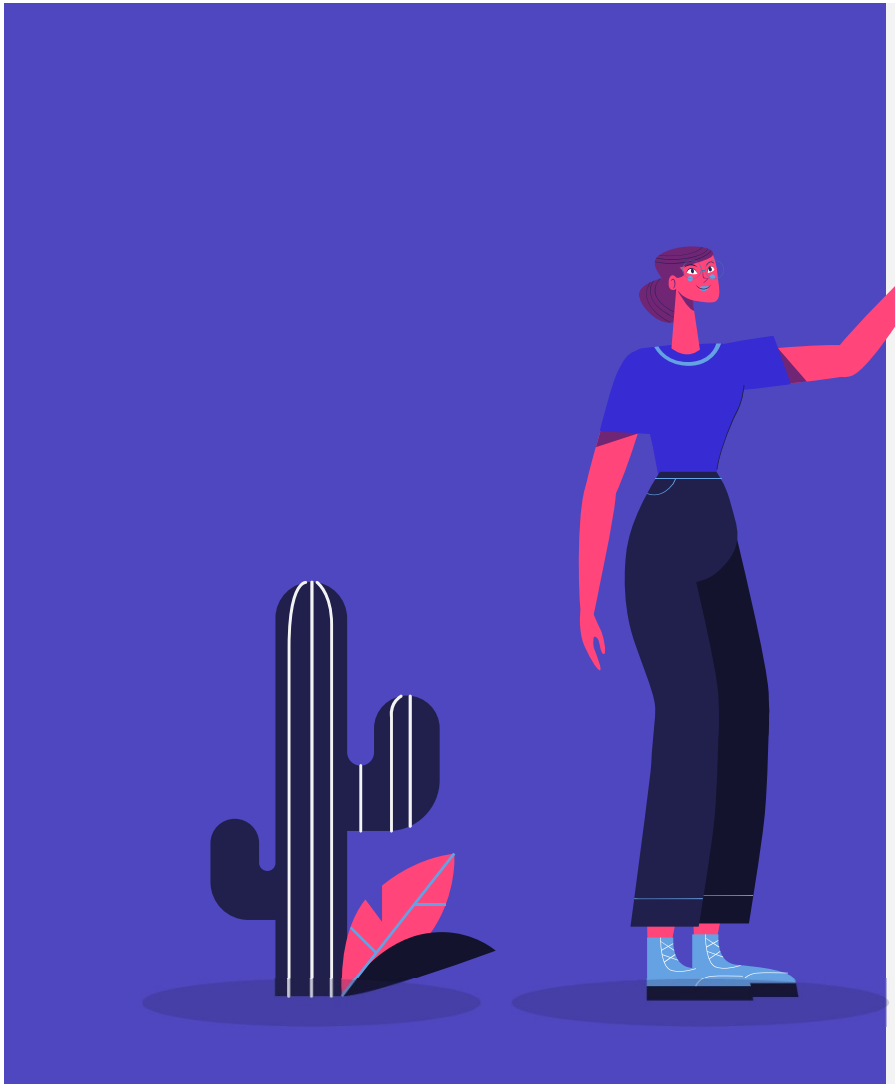

Bedreiging cybercrime per sector
39%
Zorg
12%
ICT
30%
Zakelijke dienstverlening
10%
Maakindustrie
Gevolgen van cybercrime
Privacyschending
Bedrijfsschade door stagnatie van processen
Eis van losgeld
Reconstructiekosten (herstel database)
(Gevoelige) informatie openbaar, beschadigd of verloren
Reputatieschade
Boete van Autoriteit Persoonsgegevens
Aansprakelijkheidsclaims
Voorbeelden van datalekken
1. Medische gegevens ingezien door onbevoegden
2. Persoonlijke gegevens van werknemers ingezien door onbevoegden (bijvoorbeeld kopieën van rijbewijzen, paspoorten, bankgegevens, wachtwoorden)
3. Verlies van een laptop met onversleutelde, financiële of anderszins gevoelige informatie
4. Een versleutelde laptop met belangrijke data is gestolen en er is geen back-up voorhanden
5. Bij een hack zijn klantgegevens en wachtwoorden ontvreemd
6. Persoonsgegevens ongeoorloofd ingezien vanwege kwetsbaarheid webapplicatie
7. Een envelop met creditcard- en/of betalingsgegevens is niet versnipperd maar in de vuilnisbak gegooid

CIJFERS

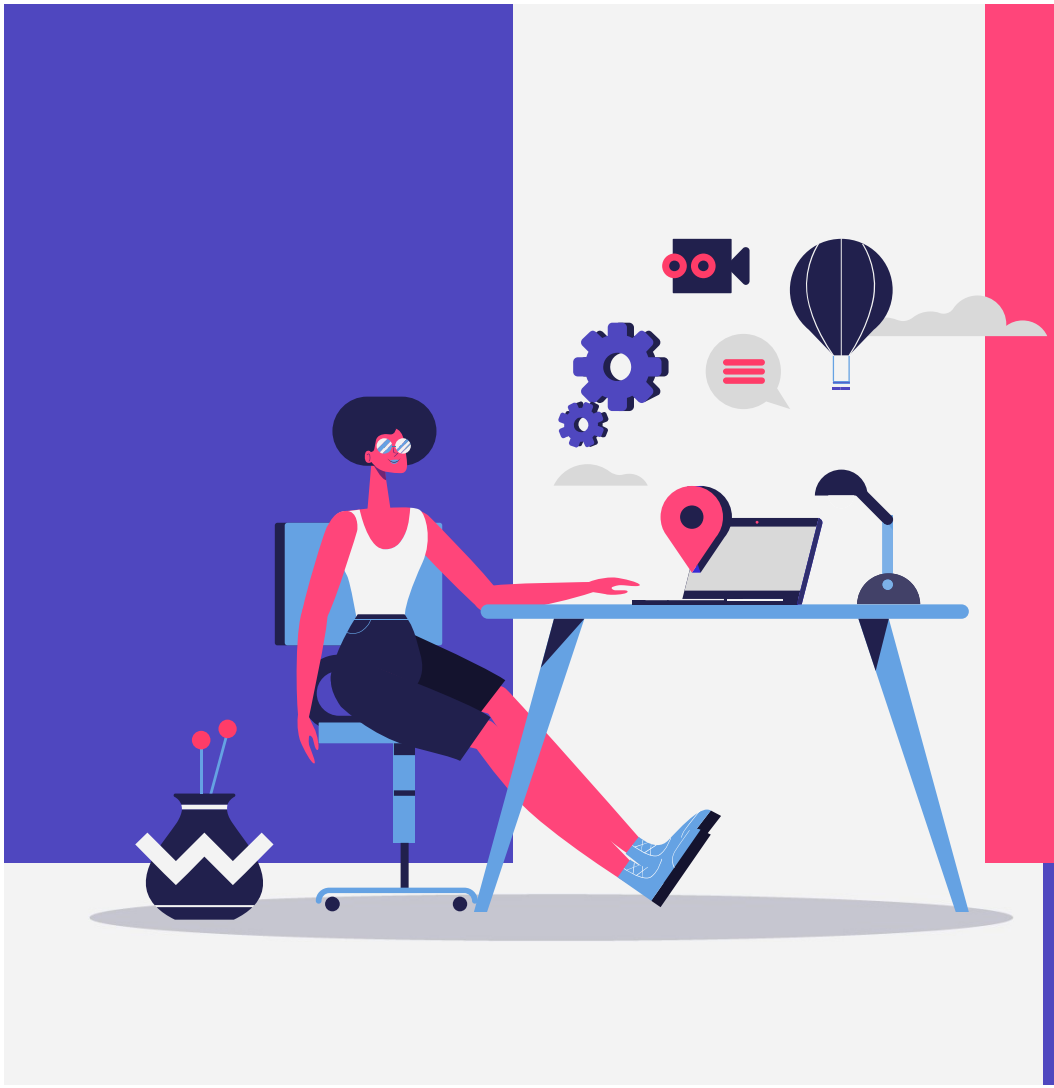
VER VAN MIJN BED?



KOST VAN EEN INCIDENT



HEB IK UW AANDACHT?



03

INCIDENTEN BEPERKEN TOT EEN MINIMUM

BEWUST INTERNET-GEBRUIK

TIPS BEWUST INTERNET-GEBRUIK

OP KANTOOR

- Incognito surfen zorgt ervoor dat je internetgedrag niet opgeslagen of in de gaten gehouden kan worden
- Dagelijks je internetgeschiedenis wissen
- Dagelijks cookies verwijderen
- Draadloze internetverbinding op kantoor goed beveiligen
- Wachtwoorden niet door je apparaat laten onthouden
- Wachtwoorden regelmatig veranderen (en niet aan derden meedelen)

OP LOCATIE

- Locatiefunctie uit te schakelen
- Niet op openbare WiFi inloggen
- Alleen inloggen op beveiligde netwerken

BEWUST E-MAIL-GEBRUIK

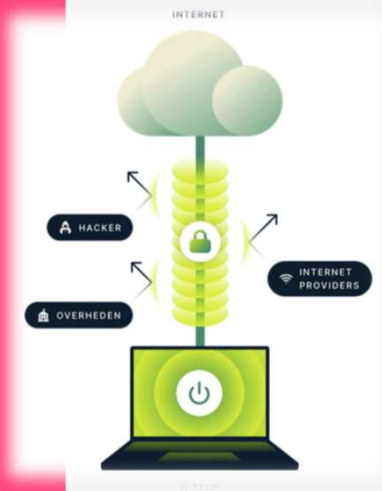
TIPS BEWUST E-MAIL-GEBRUIK

OP KANTOOR

- Onnodig gebruik van e-mail vermijden
- Wachtwoorden niet door je apparaat laten onthouden
- Wachtwoorden regelmatig veranderen (en niet aan derden meedelen)
- E-mail enkel voor het werk gebruiken
- Verzend vertrouwelijke, gevoelige of in een ander opzicht beschermde informatie geëncrypteerd
- Opletten voor het openen van e-mail met attachment (zie verder)
- Let steeds op de afzender van het mailbericht (zie verder)

OP LOCATIE

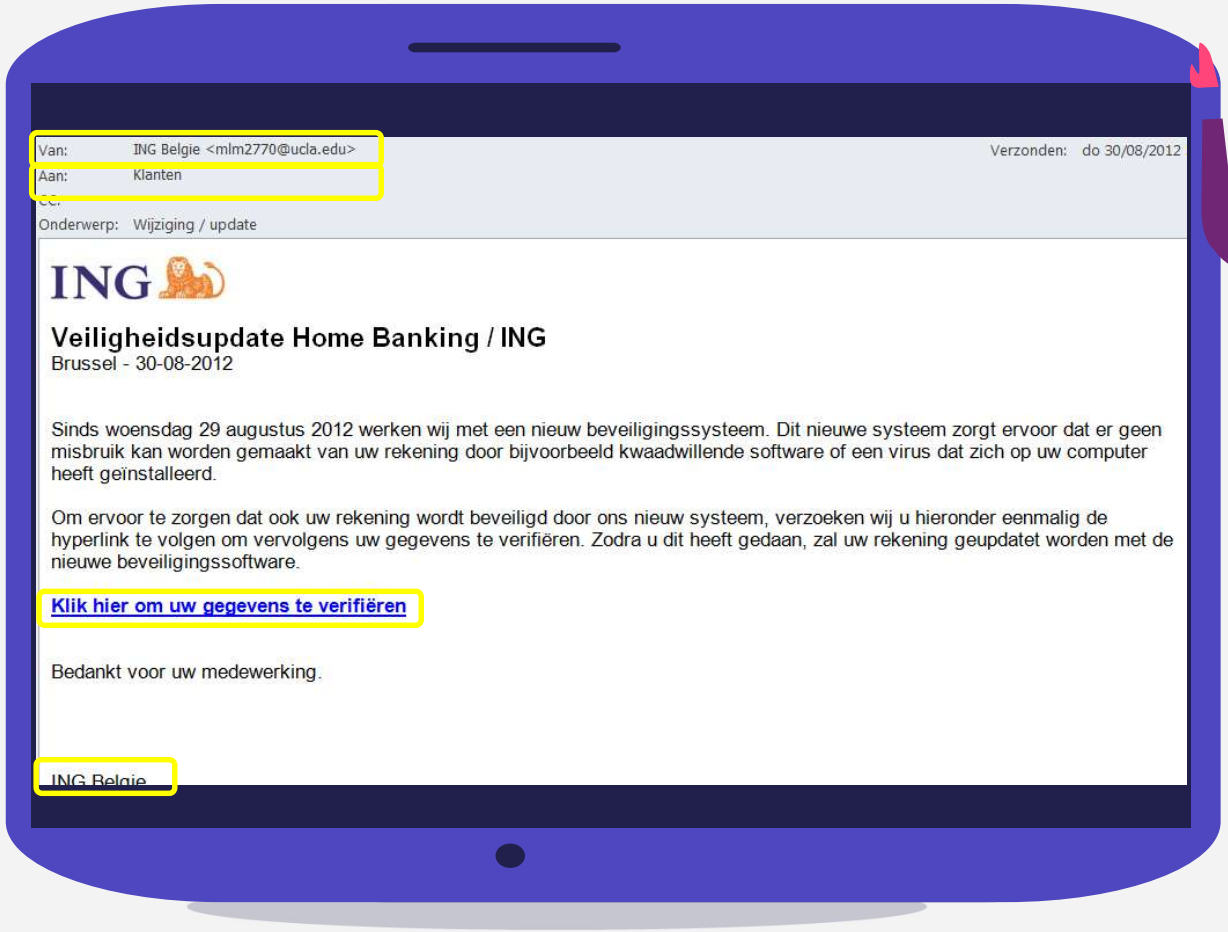
- Zie “op kantoor” +
- Gebruik VPN
  - Je bent extra beschermd online
  - Je kunt anoniem gebruik maken van het internet
  - Tijdens het downloaden ben je anoniem en veilig
  - Je kunt de censuur van andere landen omzeilen
  - Je kunt toegang krijgen tot locatie-specifieke websites en services
  - Je kunt veilig gebruik maken van openbare wifi-netwerken



STERKE WACHT-WOORDEN

HOE SNEL KAN EEN WACHTWOORD GEKRAAKT WORDEN?

Tekens	Aantal mogelijke combinaties	Brute force tijd
1	62	direct
2	3,844	direct
3	238,328	direct
4	14,776,336	direct
5	916,132,832	42 seconden
6	56,800,235,584	43 minuten
7	3,521,614,606,208	44 uur
8	218,340,15,584,896	115 dagen
9	13,537,086,546,263,600	20 jaren
10	839,299,365,868,340,000	12 eeuwen



PHISHING-MAILS KLEINE TEST

TIPS

Bejegening

Word je persoonlijk aangesproken of is de aanspreking ‘algemeen’?

Let op taalfouten

Afzender?

Let op het mailadres van de afzender (bijvoorbeeld: INGbank_@outlook.com)

Verdachte bijlagen

Als het bestand eindigt op bijvoorbeeld .exe of .zip, is het wellicht niet te vertrouwen. Ook Pdf-bestanden kunnen al schadelijke inhoud bevatten

Vraag naar persoonsgegevens

Mocht je naar aanleiding van een ontvangen bericht willen inloggen op een website, klik dan nooit op links in de e-mail

Opvallende links

Op het moment dat je met je muis over de link zweeft kan je vaak links onderin je browser zien naar welke internetadres de link echt verwijst

Volg je intuïtie!

Wees liever één keer te voorzichtig dan één keer te roekeloos.

Bij twijfel, neem contact op met de organisatie via een telefoonnummer of e-mailadres dat je 100% zeker vertrouwt

VERDACHTE BESTANDSTYPEN

.bat (Batch)	**.com** (COM bestand)	**.cpl** (Control Panel)
.docm (Microsoft Word met macro's)	**.exe** (Windows Executable bestand)	**.jar** (Java)
.js (JavaScript)	**.pif** (Programma Informatie bestand)	**.pptm** (Microsoft PowerPoint met macro's)
.ps1 (Windows PowerShell)	**.scr** (Screensaver bestand)	**.vbs** (Visual Basic Script)
.wsf (Windows Script File)	**.xlsm** (Microsoft Excel met macro's)	**.zip (Compressed)**

Wordt best veel gebruikt -> beter delen via een SharePoint of OneDrive

BEWUST SOCIAL MEDIA GEBRUIK

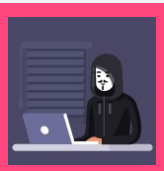
TIPS BEWUST SOCIAL MEDIA GEBRUIK

OP KANTOOR

- Is het toegestaan om tijdens het werk actief zijn op sociale media mits het werk gerelateerde content betreft?
- Deel geen sociale media berichten (ook geen links)
- Gebruik zeker geen sociale media om (gevoelige) werk gerelateerde zaken te delen (Messenger, Whatsapp...)
- Maak een onderscheid tussen professioneel en persoonlijk gebruik

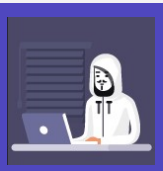
04 HACKERS @ WORK

2 SOORTEN HACKERS



BLACK HAT HACKER

- iemand die de beveiliging en integriteit van computers of netwerken schendt met malicieuze intenties of voor persoonlijk gewin
- breken in op computersystemen met het doel om daar zelf voordeel uit te halen
- breken in bij beveiligde netwerken om data te vernietigen, te bewerken of te stelen
- zorgen er dikwijls voor dat anderen niet meer op reguliere wijze gebruik kunnen maken van een netwerk



WHITE HAT HACKER

- Computerbeveiligingsspecialist
- gebruiken vaak dezelfde technieken om in te breken op computers en netwerken
- verschil zit in de intenties
- proberen beveiligingslekken op te sporen en assisteren bij het zoeken naar oplossingen om de beveiliging te verbeteren

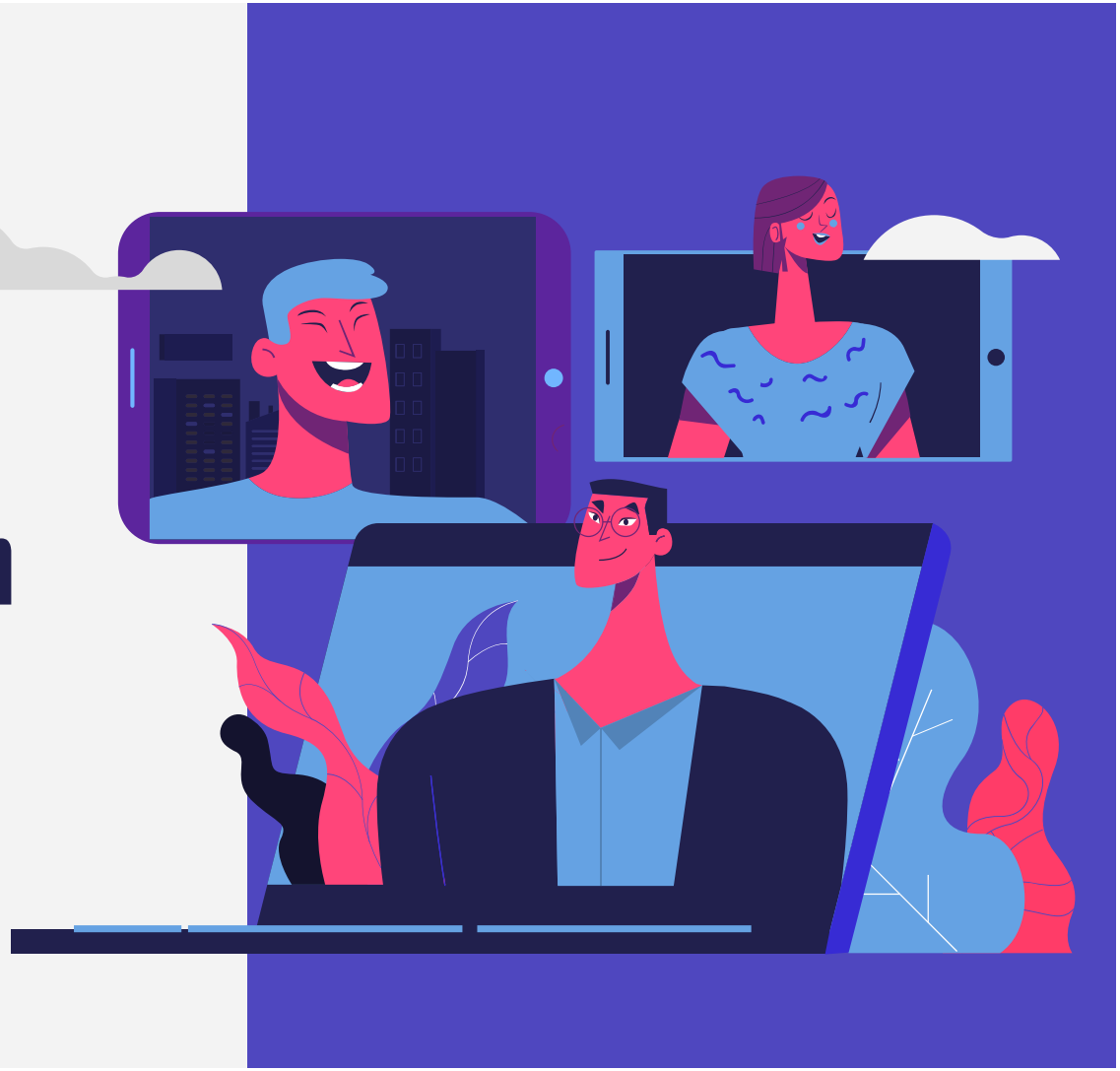
WELKE TOOLS GEBRUIKEN ZE?

- Web vulnerabilty scanners (spiders)
- Network Discovery & Security Auditing
- Port scanners
- Forensic tools
- Password cracking tools
- Firewall crackers
- WiFi hacking tools
- Social engineering Toolkits
- ...

Zoals:

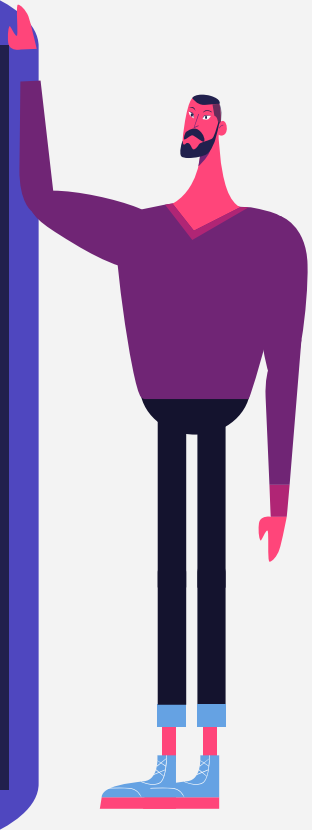
- zoals:
- Acunetics WVS
- Nmap
- Wireshark
- oclHashcat
- Nessus VS
- Maltego
- Netsparker
- W3af
- ...

Wat ingeval van een datalek?



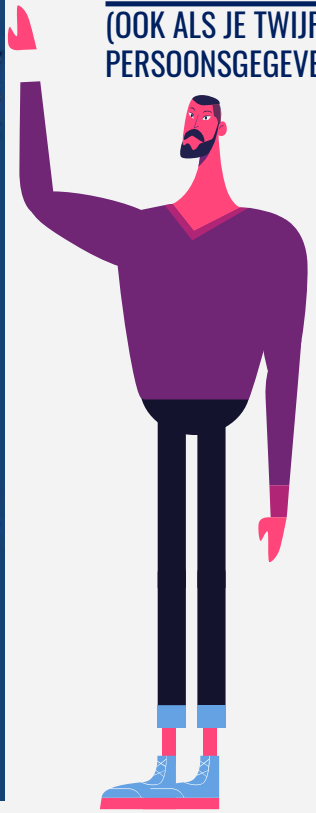
WAT ZEGT DE WET?

- er sprake is van een datalek als er een “risico voor de rechten en vrijheden van de betrokkene” bestaat
- verplichting om het gegevenslek mee te delen aan de betrokkene, wanneer er sprake is voor een hoog risico voor de betrokkene
- melding moet gebeuren door de verwerkingsverantwoordelijke, of door de verwerker indien de verwerkingsverantwoordelijke hierover expliciet schriftelijke afspraken heeft gemaakt met de verwerker
- de meldingstermijn bedraagt maximaal 72 uur nadat het gegevenslek werd **vastgesteld**
- zelfs indien de verwerkingsverantwoordelijke het gegevenslek niet meldt bij de Autoriteit, houdt hij best toch een logboek bij van incidenten. Dit bevat best een korte beschrijving van elk gegevenslek en een verklaring voor het niet-melden ervan.

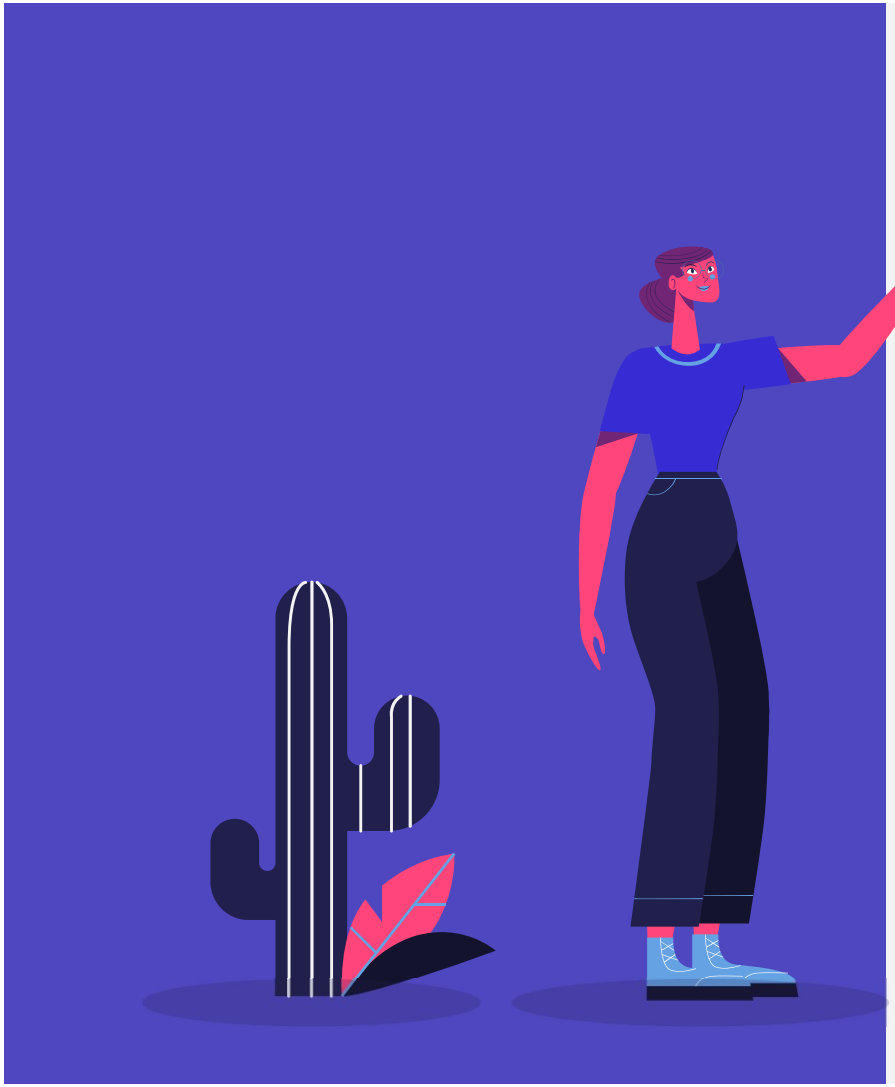


STEEDS EN ONMIDDELLIJK MELDEN

(OOK ALS JE TWIJFELT en OOK ALS HET NIET OVER PERSOONSGEGEVENS ZOU GAAN...)



WAT TE DOEN BIJ EEN DATALEK?



Lexit
lawyers and consultants
at privacy law

VRAGEN?

Dupont Diego
diego.dupont@gdprmasters.com
0491-63.06.67