Een datalek, wat nu?

Een praktische vertaling van juridische vereisten

Donderdag 3 oktober 2019

mr. Peter Kager

CIPP/E & CIPT

Directeur ICTRecht Privacy

1

Hoe ver mag een sportclub gaan om de beste prestaties uit zijn spelers te halen? In België zijn de meningen hierover verdeeld.

Spelers van Belgische voetbalclub KRC Genk kregen van hun club allemaal een polsband met een *activity tracker*. Het is de bedoeling dat zij die buiten de training dragen, zodat hun slaapritme, lichaamsherstel en algemene inspanning gemeten kan worden. Met die data kan de training voor elke speler gepersonaliseerd worden.

2

3

AVG

Van toepassing op:

- Geheel of gedeeltelijk geautomatiseerde verwerking;
- Niet geautomatiseerde verwerking, maar opgenomen in bestand (gestructureerd geheel en systematisch toegankelijk).

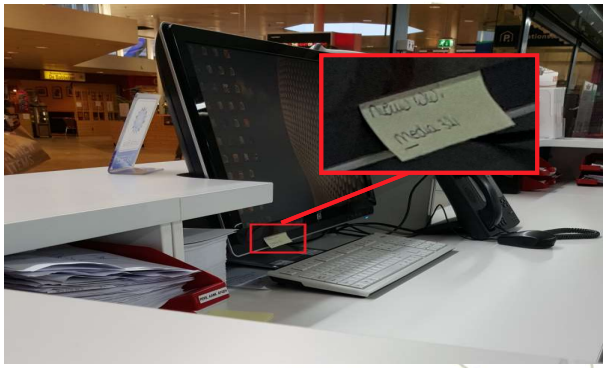
Niet van toepassing op:

- Handmatige ongeordende verwerking;
- Persoonlijke of huishoudelijke doeleinden;
- Politie, inlichtingen en veiligheidsdiensten;
- Wet GBA;
- Wet justitiële en strafvorderlijke gegevens;
- Kieswet;
- Krijgsmacht;
- Journalistieke doeleinden.

4

DATALEKKEN

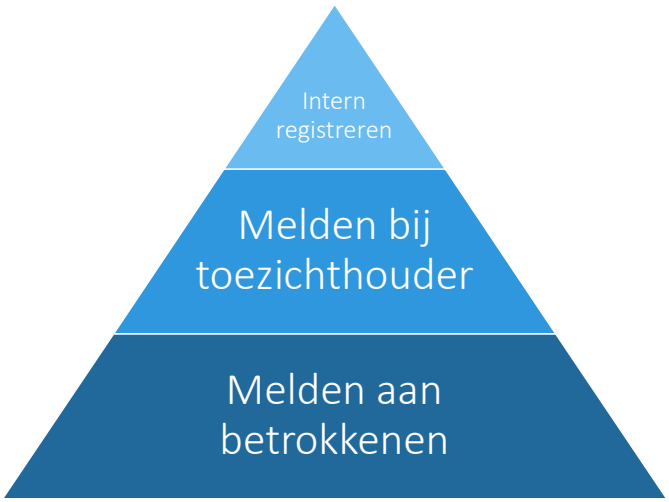
Iedere inbreuk op de beveiliging die **per ongeluk of op onrechtmatige wijze** leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens;



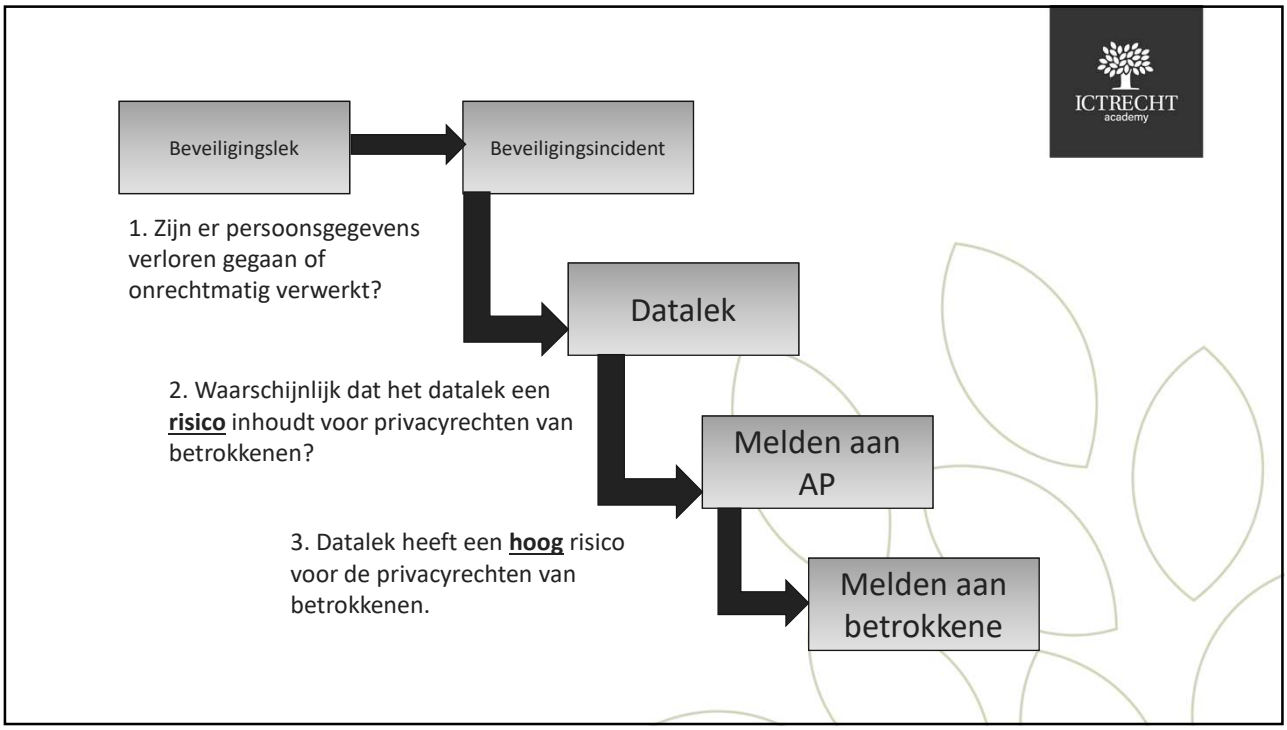
Art. 4 lid 12 AVG

5

DRIE ACTIES BIJ DATALEKKEN



6



7

MELDEN AAN TOEZICHTHOUDER

AUTORITEIT PERSOONSGEGEVENS

- Direct, en uiterlijk binnen 72 uur, aan toezichthouder melden:
  - Aard van de inbreuk;
  - Soorten en hoeveelheid data;
  - Contactinformatie;
  - Aanbeveling ter beperking vervolgschade;
  - Gevolgen schetsen.
- Documenteren

Art. 33 AVG

8

ALTIJD MELDEN AAN TOEZICHTHOUDER, TENZIJ….

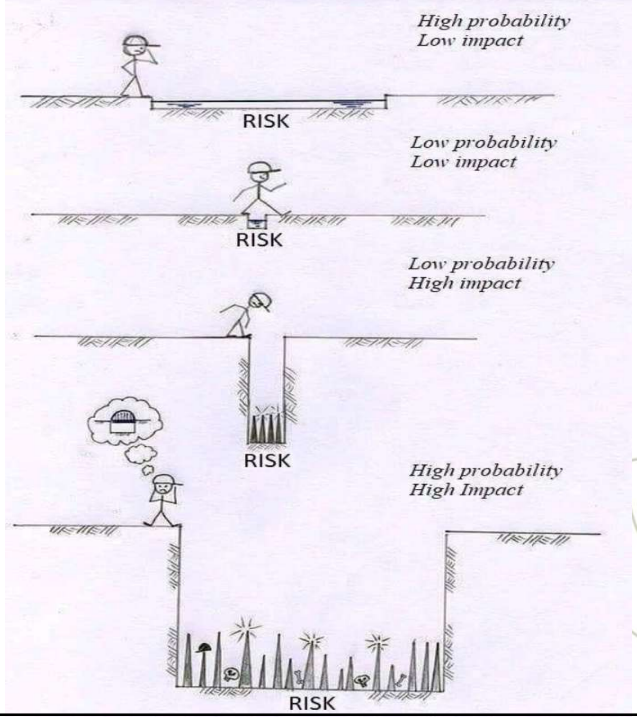
AUTORITEIT PERSOONSGEGEVENS

Een melding kan achterwege blijven wanneer het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen.

Art. 33 AVG

9

RISICO'S



10

BEOORDELING VAN RISICO'S

- De aard van de inbreuk: wat is er gebeurd (verlies, wijziging van gegevens)?
- De aard, gevoeligheid en omvang van de persoonsgegevens: hoe gevoeliger de gegevens, hoe groter het risico;
- Gemak waarmee personen kunnen worden geïdentificeerd;
- Ernst van gevolgen voor personen: identiteitsdiefstal of reputatieschade;
- Bijzondere kenmerken van de persoon: bijvoorbeeld kwetsbare groepen, zoals kinderen;
- Bijzondere kenmerken van uw organisatie: ziekenhuis / overheid zal snel moeten melden;
- Het aantal getroffen personen.

11

MELDEN BIJ DE AUTORITEIT PERSOONSGEGEVENS

Gegevens van gevoelige aard:

- Bijzondere persoonsgegevens;
- Gegevens over financiële of economische situatie betrokkene;
- Gegevens die kunnen leiden tot stigmatisering of uitsluiting van de betrokkene (gokverslaving, werkprestaties, relatieproblemen);
- Gebruikersnamen, wachtwoorden en andere inloggegevens;
- Gegevens die kunnen worden misbruikt voor (identiteits)fraude (biometrische gegevens, BSN, kopie ID-bewijs).

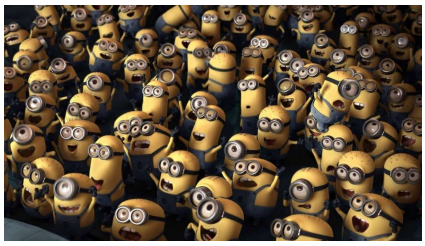
Aard en omvang van de inbreuk:

- Databases met persoonsgegevens van grote groepen mensen;
- Mate van gebruik van persoonsgegevens;
- Overheidsverwerkingen;
- Verlies NAW-gegevens in specifieke gevallen.

12

13

MEDEDELEN AAN BETROKKENEN



- Wanneer het lek waarschijnlijk een hoog risico inhoudt voor de betrokkenen
- Onverwijld melden
- In begrijpelijke taal (B2!):
  - Contactinformatie
  - Aanbeveling ter beperking vervolgschade
  - Gevolgen schetsen

Art. 34 AVG

14

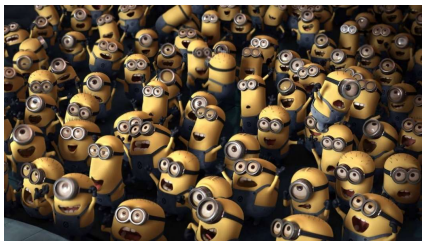
HOOG RISICO

Beoordeling van risico's:

- Discriminatie: bijvoorbeeld bij een datalek met gegevens over ras, geloof of seksuele geaardheid.
- Identiteitsdiefstal of –fraude: bijvoorbeeld bij een datalek met complete paspoortkopieën. Of het BSN in combinatie met andere persoonsgegevens.
- Financiële verliezen: bijvoorbeeld bij een datalek met creditcardgegevens waardoor het risico bestaat dat iemand online bestellingen kan plaatsen op kosten van een ander.
- Reputatieschade: bijvoorbeeld bij een datalek met gegevens over problematische schulden, verslaving of prestaties op het werk.
- Doorbreking van beroepsgeheim: bijvoorbeeld bij een datalek met medische gegevens.

15

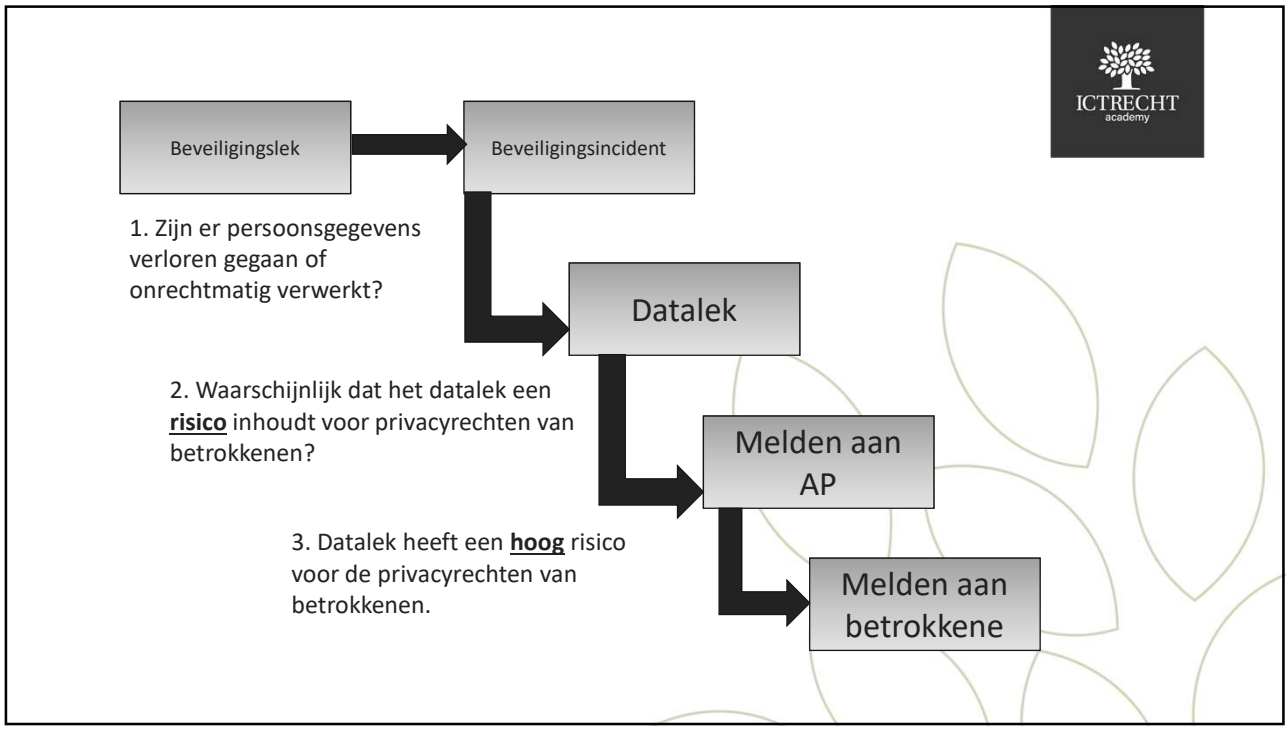
UITZONDERING



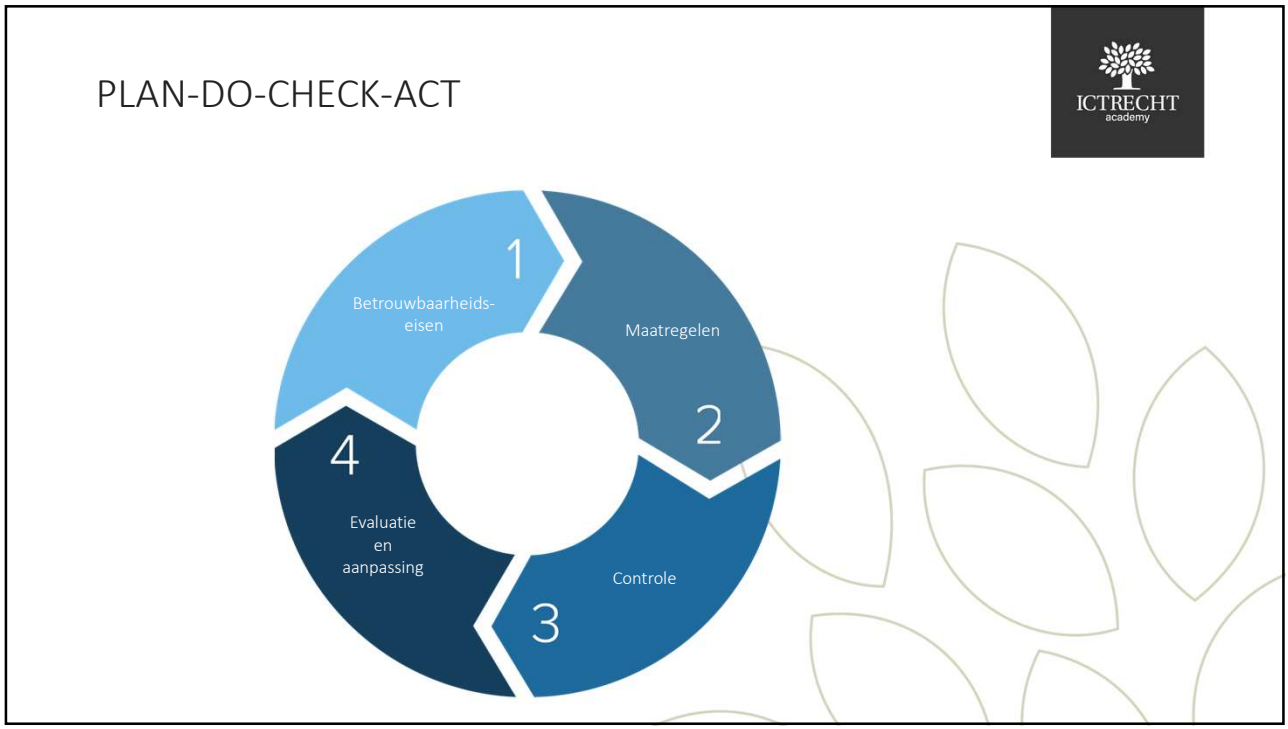
- Er passende technische en organisatorische maatregelen zijn genomen die data **onbegrijpelijk** maken voor onbevoegden;
- Verantwoordelijke nadelige gevolgen voor betrokkenen direct wegneemt;
- Een individuele melding buitenproportioneel is. In dat geval volstaan een publieke mededeling (bijvoorbeeld op website).

Art. 34 lid 3 AVG

16


Beveiligingslek
Beveiligingsincident
1. Zijn er persoonsgegevens verloren gegaan of onrechtmatig verwerkt?
Datalek
2. Waarschijnlijk dat het datalek een **risico** inhoudt voor privacyrechten van betrokkenen?
Melden aan AP
3. Datalek heeft een **hoog** risico voor de privacyrechten van betrokkenen.
Melden aan betrokkene

17


PLAN-DO-CHECK-ACT
1
Betrouwbaarheids-eisen
Maatregelen
2
4
Evaluatie en aanpassing
Controle
3

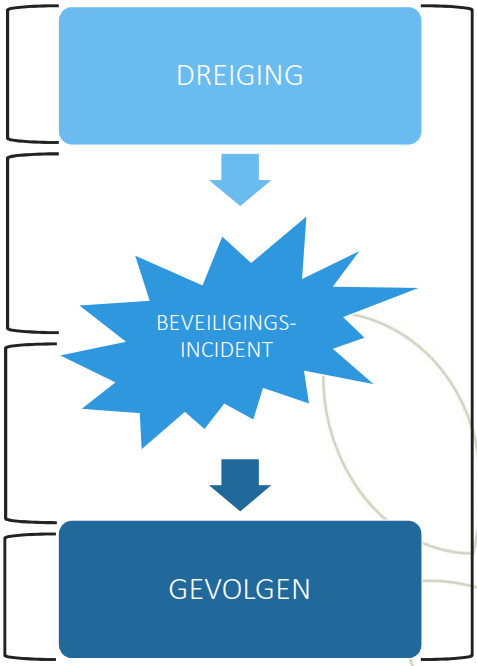
18

Preventieve maatregelen
Voorkomen dat een dreiging leidt tot een beveiligingsincident

Detectieve maatregelen
Weten dat er een beveiligings-incident heeft plaatsgevonden

Repressieve maatregelen
Beperken van de negatieve gevolgen van het beveiligings-incident

Herstelmaatregelen
Verhelpen van de negatieve gevolgen



Correctieve maatregelen
Repareren van de gebleken tekortkomingen in de beveiliging

19

REGISTER VAN DATALEKKEN

- Documenteren van *alle* datalekken binnen organisatie
- Mag elektronisch beheerd
- Zowel voor verwerker als voor verantwoordelijke verplicht

➢ Inzageplicht op verzoek van toezichthouder

Art. 33 AVG

20

WAT TE DOEN TEGEN DATALEKKEN?

1. Maak beleid over interne doorgifte datalekken en besluitproces melding toezichthouder
2. Werk beleid uit tot concrete procedures en toets de uitvoering
3. Dwing bij leveranciers van tools garanties af over datalekken
   - Verhoog hun aansprakelijkheid voor bugs die datalekken veroorzaken
   - Laat ze opdraaien voor de kosten van een security audit.
4. Herzie verwerkersovereenkomsten ten aanzien van datalekken
5. Audit jezelf

21

VRAGEN OM TE STELLEN BIJ DATALEKKEN

Do's

- Wat zijn de feiten?
- Welke personen zitten er in het calamiteitenteam en wie heeft de leiding?
- Gaan we externe hulp inschakelen?
- Wat is het beste voor de 'slachtoffers'?

En:

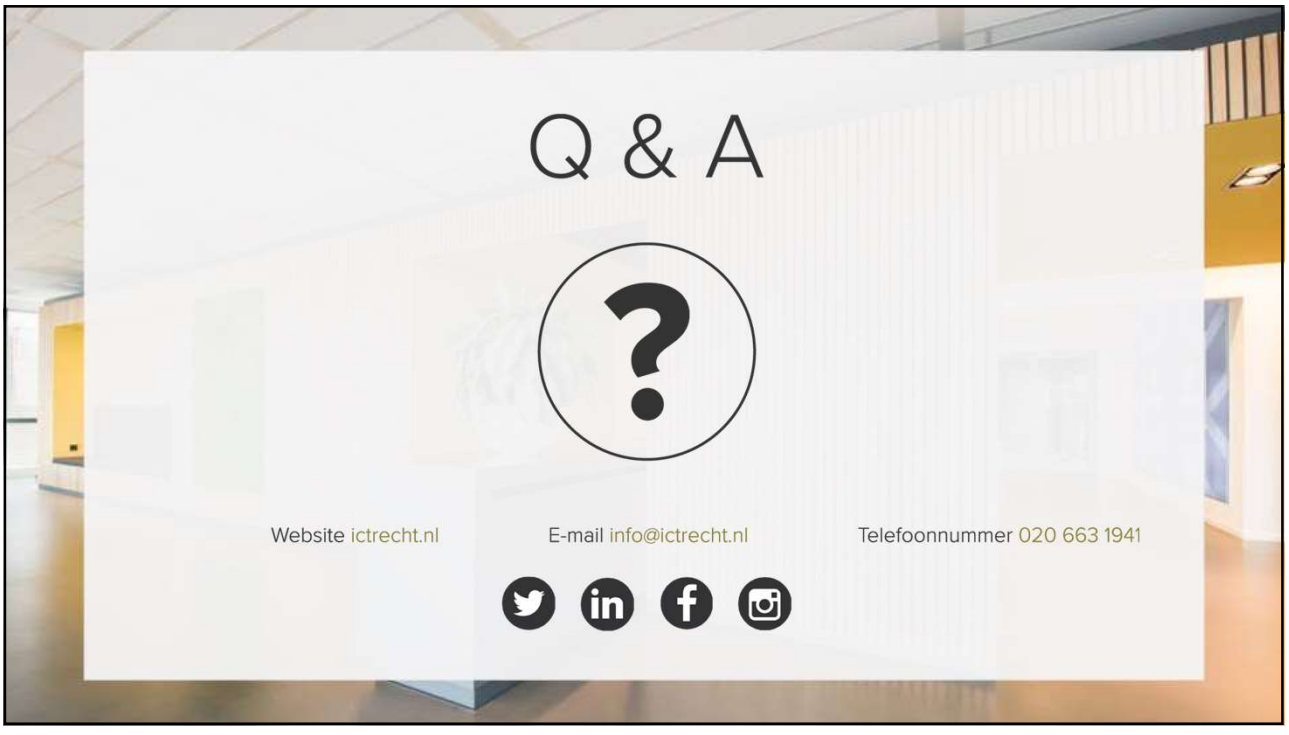
- Moeten we dit wel op schrift hebben?
- Wat vinden de aandeelhouders?

22

WAT NIET TE DOEN BIJ DATALEKKEN?

- Trek geen overhaaste conclusies onder tijdsdruk;
- “Ze komen er toch nooit achter”;
- Vergeet de contractuele afspraken niet;
- Vergeet niet te leren van het datalek!

23



24