Wet Bescherming Persoonsgegevens & Testen

1

Agenda

- Wet Bescherming Persoonsgegevens
- Risico's en Gevolgen voor Testactiviteiten
- Oplossingsrichtingen voor testdata

2

Maar eerst. . .

- Juridische bronnen:
  - Formeel
  - Correct
  - Vaag
  - Onbegrijpelijk voor leken
  - Langdradig
  - Saai

- Als je dit aantrekkelijk vindt klinken:
  - kom naar de KZA-stand, of
  - mail me (eploum@kza.nl)

3

Wet Bescherming Persoonsgegevens (WBP)

4

Wet Bescherming Persoonsgegevens

- Sinds 1 september 2001
- Vervanging Wet Persoonsregistratie (WPR)
- Handhaving door College Bescherming Persoonsgegevens (CBP)

5

Wet Bescherming Persoonsgegevens

- Beveiliging van het (automatische) *verwerken*, *verzamelen* en *vernietigen* van *persoonsgegevens*,
- door middel van *technische* en *organisatorische maatregelen*,
- met het oog op waarborging van *exclusiviteit, integriteit* en *continuïteit*.

6

Loopt het zo'n vaart?

- Komt u tijdens het testen in aanraking met:
  - Persoonsgegevens die niet publiek toegankelijk zijn? (bijv. lidmaatschappen, overeenkomsten etc.)

→ **WBP van toepassing**

7

Loopt het zo'n vaart?

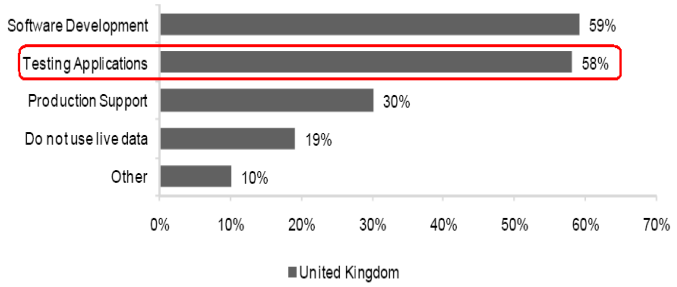
- Komt u tijdens het testen in aanraking met:
  - **Bankgegevens**
  - **Verzekeringsgegevens**
  - Gegevens die onder een formele geheimhouding vallen (bijv. medische of strafrechtelijke informatie)
  - **Politieke voorkeur, ras, religie, seksueel leven, lidmaatschap vakvereniging**

→ **Voor testen mogen slechts *fictieve* gegevens gebruikt worden**

8

Loopt het zo'n vaart?

Does your organization use live data for procedures such as production support, testing applications and software development (more than one response allowed)?



Bron: Ponemon Institute LLC (sponsored by Compuware), *The Insecurity of Test Data: The Unseen Crisis* (United Kingdom Survey), January 31 2008

9

Loopt het zo'n vaart?

➢ Persbericht CBP 28 januari 2008:

➢ "In antwoord op die ontwikkelingen heeft het CBP er voor gekozen om veel meer dan voorheen gebruik te maken van zijn handhavende bevoegdheden. Met indringend, soms ook onaangekondigd onderzoek naar overtredingen van de privacyregels op basis waarvan zo nodig gedreigd kan worden met (hoge) boetes, is de bijdrage aan de naleving van de wettelijke verplichtingen door overheid en bedrijfsleven naar het oordeel van het CBP het grootst."

10

Loopt het zo'n vaart?

CBP legt last onder dwangsom op aan vier ziekenhuizen

Informatiebeveiliging ziekenhuizen niet op orde

Persbericht, 8 juni 2009
Het College bescherming persoonsgegevens (CBP) maakt vandaag bekend dat het vier ziekenhuizen een last onder dwangsom oplegt na onderzoek naar de informatiebeveiliging in de ziekenhuizen. Volgens het CBP handelen de ziekenhuizen in strijd met de Wet bescherming persoonsgegevens (Wbp) doordat het niveau van informatiebeveiliging niet voldoet aan de daarvoor geldende norm. Met name het ontbreken van kennis over waar men welke risico's loopt op het gebied van informatiebeveiliging rekent het CBP de ziekenhuizen aan. Dit kan namelijk ernstige gevolgen hebben voor de kwaliteit van de zorg en de privacy van patiënten. Het betreft Ommelander Ziekenhuis Groep, MC/Lelystad, Medisch Spectrum Twente en het Rijnland Ziekenhuis. Over een vijfde aangesproken ziekenhuis, het Diaconessenhuis Leiden, heeft het CBP besloten om af te zien van het opleggen van een last onder dwangsom, onder meer omdat dat ziekenhuis inmiddels wel beschikt over een adequate risicoanalyse.

Bron: http://www.cbpweb.nl/Pages/pb_20090608_lod_ziekenhuizen.aspx

11

Loopt het zo'n vaart?

- OPTA boetebeleid, klasse **zware overtredingen**
  - "*Overtreding van de verplichtingen die strekken tot bescherming van persoonsgegevens en de persoonlijke levenssfeer (artikel 11.2 Tw en artikel 11.3, eerste lid);*"

12

Context

13

Verantwoordelijke

- Meldingsplicht aan CBP (of functionaris)
  - Vrijstellingsbesluit Artikel 33 niet bruikbaar voor testen
- Informatieplicht aan Betrokkene
  - Melden waarvoor de gegevens gebruikt worden
  - Betrokkene heeft recht op inzage
  - Betrokkene heeft recht op correctie
- ‘Passende technische en organisatorische beveiligingsmaatregelen’ die een ‘passend beveiligingsniveau’ garanderen

14

‘Passende Beveiligingsmaatregelen’

- Niet gespecificeerd door wetgever
- Criteria:
  - Stand van de techniek
  - Kosten
  - Gevoeligheid van de gegevens
  - Gevoeligheid context waarin de gegevens gebruikt worden
- Periodieke heroverweging is dus nodig

15

Verantwoordelijke

- Gegevens niet langer bewaren dan noodzakelijk
  - Vrijstellingsbesluit Artikel 33 vereist dat voor vrijstelling van de meldingsplicht de gegevens niet langer bewaard worden dan *6 maanden* na verkrijging.
- Software van derden moet worden goedgekeurd en voldoen aan beveiligingseisen

16

Bewerker

- WBP eisen aan overeenkomst verantwoordelijke en bewerker:
  - *Waarborging* voldoende technische en organisatorische beveiliging
  - Afdwingbare verbintenissen
  - Bewerker werkt alleen *in opdracht* van verantwoordelijke
  - Bewerker moet dezelfde *beveiligingsverplichtingen nakomen* als de verantwoordelijke volgens de WBP heeft
  - Verantwoordelijke moet *toezien op de naleving* van de beveiligingsverplichting

17

Bewerker

Bewerker is aansprakelijk voor schade die gevolg is van zijn bewerkingshandelingen

18

Dus…

Bron: www.nu.nl

België betaalt per ongeluk te veel uitkeringen

Uitgegeven: 22 oktober 2009 10:18
Laatst gewijzigd: 22 oktober 2009 10:18

BRUSSEL - Een test van een nieuw betaalprogramma bij een Belgische werkloosheidsuitkering blijkt verkeerd te zijn afgelopen. Door een foutje is daadwerkelijk 40 miljoen euro aan uitkeringen overgeboekt.


© ANP

De instanties doen nu alle moeite om het geld terug te vorderen van 48.860 werklozen.

De zogeheten Hulpkas voor Werkloosheidsuitkeringen had vorige week donderdag een betaalbestand met een aantal overschrijvingen gestuurd naar De Post, die de betalingen verricht voor de instelling.

Telefoontjes

Dat was bedoeld als test voor de overgang naar de Europese overschrijvingsmodellen. Maar de betaling was echt uitgevoerd, zo bleek maandag toen verraste werklozen opbelden.

De Post heeft nu een brief gestuurd met uitleg, meldde de woordvoerder van De Post donderdag. Het geld wordt automatisch van de rekeningen afgeschreven.

© ANP

19

Overeenkomst voor Verwerking Persoonsgegevens

- Risicoklasse I
  'normale', maar niet-publieke informatie
  - Procedures rond autorisaties
  - Logbestanden bijhouden
  - Opslag gegevensdragers
  - Verstrekking persoonsgegevens aan derden
  - Geheimhoudingsclausule

20

Overeenkomst voor Verwerking Persoonsgegevens

- Risicoklasse II
  gevoelige informatie
  - Jaarlijkse, steeksproefgewijze controle op beveiligingsbeleid bij bewerker
  - Jaarlijkse rapportage hiervan
- Risicoklasse III
  hooggevoelige informatie
  - Overeenkomst over en controle op specifieke beveiligingsmaatregelen bij bewerker

21

WBP: Risico's en Gevolgen voor Testactiviteiten

22

Onze klanten: de verantwoordelijken

- Moeten gegevensverwerkingen melden
- Moeten passende technische en organisatorische maatregelen en beleid vaststellen en handhaven
- Moeten bewerkers controleren
- Lopen risico op boetes als ze dit niet doen
- . . .

23

Testorganisaties: de bewerkers

- Krijgen te maken met organisatorisch beveiligingsbeleid van onze klanten
- Krijgen te maken met technische beveiligingsmaatregelen
- Mogen (in veel gevallen) alleen nog *fictieve* testdata gebruiken
- Worden verantwoordelijk gehouden voor de schade die door hun toedoen wordt aangericht

24

Testorganisaties: de bewerkers

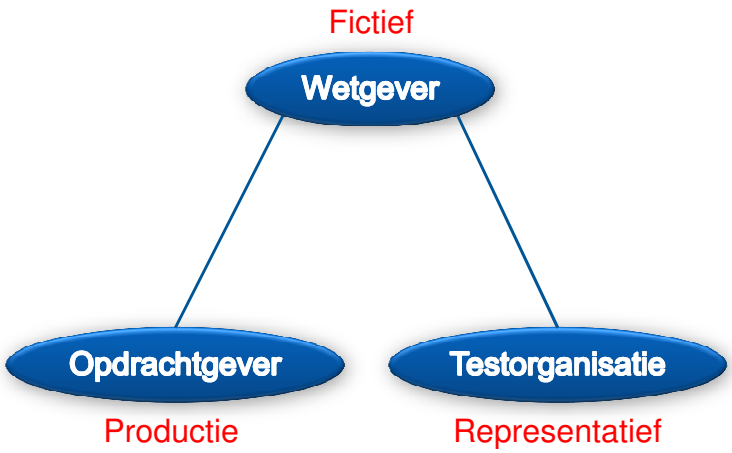
- Mogen alleen *precies* doen wat gespecificeerd staat in de overeenkomst
- Gegevens moeten vernietigd worden volgens vernietigingsprotocol en dit wordt geadministreerd
- Moeten aan het einde van de dag alle dragers van testdata in een afgesloten ruimte met inbraakdetectie opbergen

25

WBP: Testdata-oplossingsrichtingen

26

De WBP spagaat



27

De vragen die dit oproept

- Is productiedata anoniem
- Is productiedata representatief
- Is fictieve data anoniem
- Is fictieve data representatief
- Is representatieve data anoniem
- Hoe kom je aan representatieve fictieve data
- Hoe kom je aan anonieme represenatieve productiedata
- Hoe . . .

28

Twee sporen. . . . . .dezelfde vragen

Productiedata

- Extraheren
  - Op basis waarvan?
  - Relevantie?
  - Relaties/samenhang!
- Transformeren
  - WBP
  - Relaties/samenhang!
- Laden
  - Relaties/samenhang!

Fictieve data

- Creëren
  - Op basis waarvan?
  - Relevantie?
  - Relaties/samenhang!
  - WBP
  - Formaten
- Laden
  - Relaties/samenhang!

29

Dezelfde vragen. . .

- Op basis waarvan
  - Testsoort
  - Testgeval
  - Programma/Applicatie
  - Business(keten)
- Relevantie
  - Welke data heb ik nodig?
  - Hoeveel data heb ik nodig (testsoort afhankelijk)

30

Dezelfde vragen . . .

- Relaties/Samenhang
  - Welke relaties zijn er (referentieël/applicatief)
  - Welke relaties zijn relevant
  - Welke samenhang met andere (externe) databronnen
- Formaten
  - Lengtes (postcode 6 of 7, telefoon 10,11,12,13, 14, 15)
  - Dataformaat (blob, packed-decimal, etc)
  - Datanotatie (1111 XX of 1111XX, +31(0)6 of +316, etc)
  - Inhoud (M/V, M/F, 0/1, hoofd- of kleine letters, diakrieten)

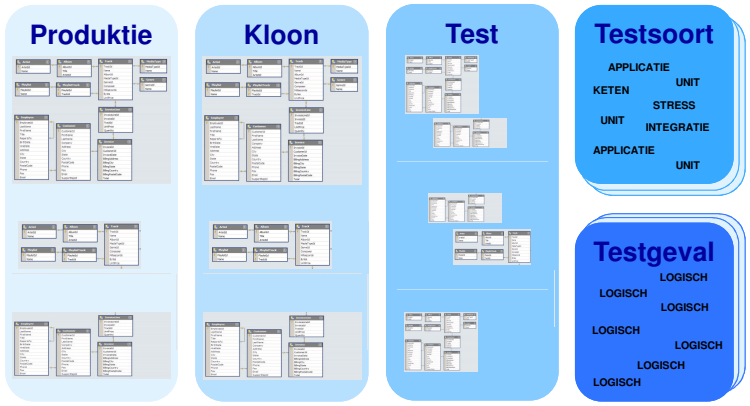
31

Dezelfde vragen . . .

- WBP
  - Anonimiseren
    - Maskeren
    - Verhaspelen
    - Verschuiven
    - Weglaten
    - Fictief
  - Strafbaar
    - Als eender welk gebruikt gegeven leidt naar een bestaand persoon.

32

Productiedata



33

Productiedata - pro's en con's

- Voordelen
  - Je weet wat je hebt:
    - Inhoud, formaat, etc
    - Relaties
    - Hoeveelheid
  - Je kan extraheren op basis van:
    - Relevantie (inhoud, testomgeving, testsoort …)
    - Quantiteit (ranges, doorsnedes, aantal …)
    - Kwaliteit? (dekking, weging, …)
- Nadelen
  - Is productie consequent en consistent?
  - Anonimiseren met behoud van consistentie en relaties
  - Hoe pas ik (voor mij) standaard privacy rules toe?
  - Wanneer ben ik WBP-proof?
  - Hoe ga ik dit onderhouden?

34

Fictieve data - pro's en con's

- Voordelen
  - Je heb (bijna) alles in de hand
    - Inhoud, formaat, Relaties, Hoeveelheid
  - Je kan creëren op basis van:
    - Relevantie. Quantiteit, Kwaliteit
- Nadelen
  - Relaties tussen verschillende databronnen (op meerdere platforms)
  - Bulk voor stress en performance
  - Hoe word ik WBP-proof?
  - Onderhoudbaarheid

35

Testdata handvatten

- Tooling
  - Data(base) schoning
  - Extractie/transformatie/laden – Subsetting/masking/rebuild
- WBP-proof
  - Minimaliseer hoeveelheid testdata
  - Wees bewust wat je wel gebruikt en waarom
  - Check connecties naar productie en externe bronnen/uitvoer
  - Virtualisatie van interne en externe bronnen buiten eigen beheer
  - Is WBP-proof mogelijk en praktisch uitvoerbaar. . . ??
- Beheer (en andere vraagstukken)
  - Vraag hulp, weinigen hebben (test)datamanagment (TDM) op orde
    - Test dienstverleners met tool en TDM kennis en kunde
    - **TestNet Werkgroep (Test)Datamanagement**

36

Presentatiebeschrijving en Korte biografieën

Presentatie

De Wet Bescherming Persoonsgegevens (WBP)wordt door veel testorganisaties niet gezien als een wezenlijke bedreiging voor hun activiteiten. Althans, dat is wat je zou kunnen afleiden uit hoe men de afgelopen 9 jaar is omgegaan met testdata. Deze wet is echter weldegelijk een risico voor de testwereld, en er zijn diverse signalen die genoeg reden geven om de WBP eens onder de loep te nemen. Deze presentatie begint met een crash-course WBP, waarna er wordt uitgelegd wat de concrete bedreigingen van deze wet zijn voor het testen. Tenslotte worden twee oplossingsrichtingen voor testdata tegen het licht van de WBP gehouden.

Ted Jans

Ik heb 30 jaar IT ervaring, voornamelijk in de IBM Mainframe omgeving. Van deze 30 jaar was ik 17 jaar actief bij de grote software-vendors van ontwikkel-, data-, monitoring- en testtools. Ik hou van de mix van het werken met tools en het spel van het overtuigen van business- en IT-mensen van de mogelijkheden en waarde van de combinatie van tools, mensen en diensten als oplossing. Als Service Ontwikkelaar bij KZA ben ik mede verantwoordelijk voor intern en extern opbouwen en uitdragen vankennis, de ontwikkeling van nieuwe producten/services en innovatie.

Eva Ploum

Ik ben afgestudeerd in de Informatica aan de Technische Universiteit in Eindhoven, en sinds een half jaar bij KZA in dienst als productontwikkelaar. Mijn specialisaties zijn het slaan van bruggen tussen mens en techniek en plaatsen van technologie in haar bredere context. Het project waar ik op dit moment aan werk betreft een innovatieve tool die relevante, representatieve en veilige testdata ondersteunt.