Developing Compliant Applications

Martin Knobloch
martin.knobloch@owasp.org

OWASP NL Chapter Board
OWASP Global Education Committee Chair

OWASP

The OWASP Foundation
http://www.owasp.org

Compliancy?

Laws and Legislations?

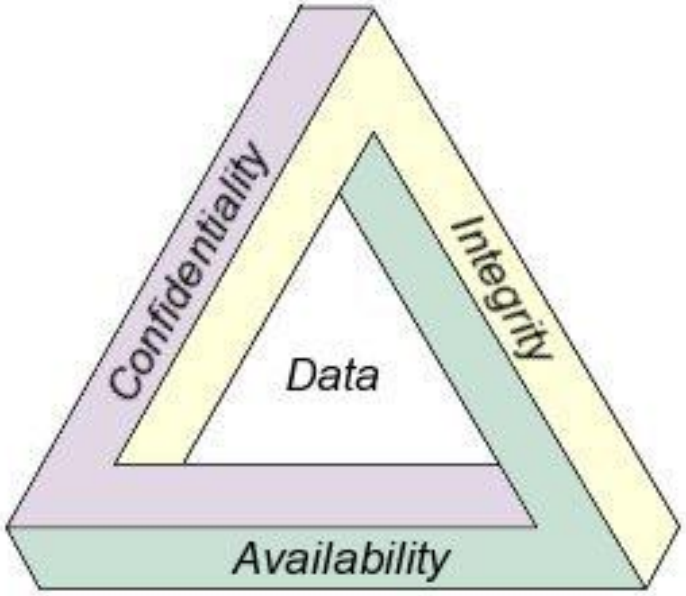
Laws are National, (web) applications are International (as is cybercrime)

The Ducht Law on Cybercrime

- 1993
  - First Law on Computer Crime
- 2001
  - Nederland does sign the Cybercrime-agreement
- 2005
  - Request for chance
- 2006
  - Approval of the current law

The Dutch National Cybercrime Legislation

1. Offences against the confidentiality, integrity, and availability of computer systems
    a) Hacking
    b) Illegal interception
    c) Data interference
    d) System interference
    e) Misuse of devices



The Dutch National Cybercrime Legislation

2. Computer-related traditional offences
    a) Computer fraud
    b) Computer forgery
    c) Data theft
    d) Identity theft
    e) Sexual offences: grooming

The Dutch National Cybercrime Legislation

3. Illegal content
    a) Child pornography
    b) Racism

4. Infringements of copyright and related rights

5. Privacy (or "data protection") offences
    a) Privacy offences
    b) Data protection offences

The Dutch National Cybercrime Legislation

6. Liability of Internet service providers

The **liability** of Internet Service Providers (ISPs) **for illegal or unlawful content** has been regulated as a consequence of the Electronic Commerce Directive. The major part concerns civil liability, as regulated in art. 6:196c of the Civil Code (*Burgerlijk Wetboek).* ***"Mere conduit" providers are not liable****; caching providers* are not liable if they do not change information and if they operate according to generally recognized procedures; and providers of information services are not liable if they have no knowledge of unlawful content and if they remove or make inaccessible the information as soon as they do gain knowledge of it.

One specific exemption from liability for ISPs has been inserted into the criminal law. Art. 54a DCC determines that intermediaries who offer a telecommunications service consisting of transport or storage of data shall not be prosecuted as such if they do all that can reasonably be asked of them to ensure that the data are made inaccessible, in response to an order from the public prosecutor. The prosecutor requires a warrant from the investigating judge for such an order, so that there is an independent check by the courts on whether the information at issue really is illegal or unlawful.

The Duty to Regulate Cybercrime Legislation

Industry Regulations

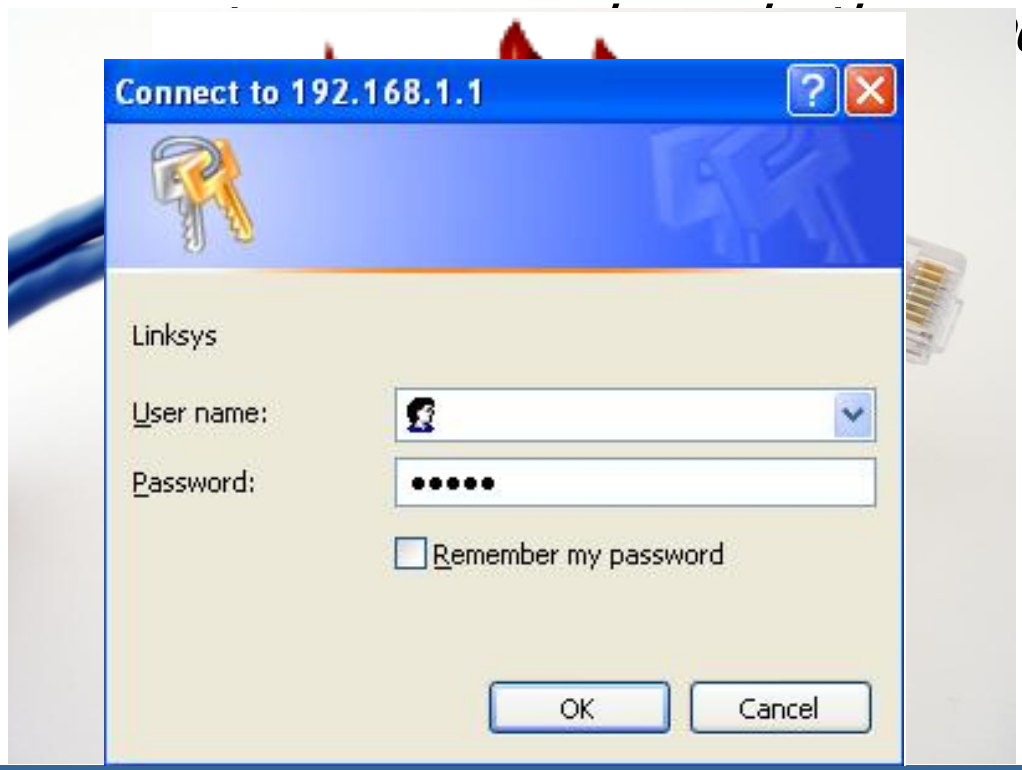
PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Build and Maintain a Secure Network

  Requirement 1: Install and maintain a firewall configuration to protect cardholder data

  Requirement 2: Do not use vendor-supplied defaults for curity parameters



PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Protect Cardholder Data

PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Protect Cardholder Data

  Requirement 3: Protect stored cardholder data

PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Protect Cardholder Data
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI – DSS

Payment Creditcard Industry Data Security Standaard

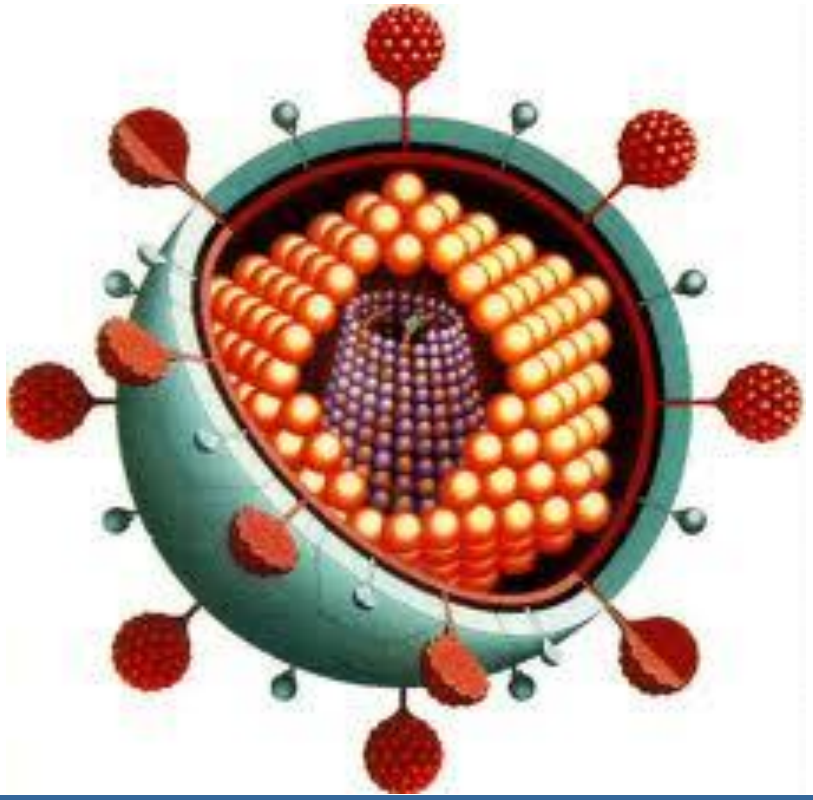
- Maintain a Vulnerability Management Program

PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Maintain a Vulnerability Management Program

  Requirement 5: Use and regularly update anti-virus software or programs



PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Maintain a Vulnerability Management Program
  - Requirement 5: Use and regularly update anti-virus software or programs
  - Requirement 6: Develop and maintain secure systems and applications

PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Implement Strong Access Control Measures

PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Implement Strong Access Control Measures

  Requirement 7: Restrict access to cardholder data by business need to know

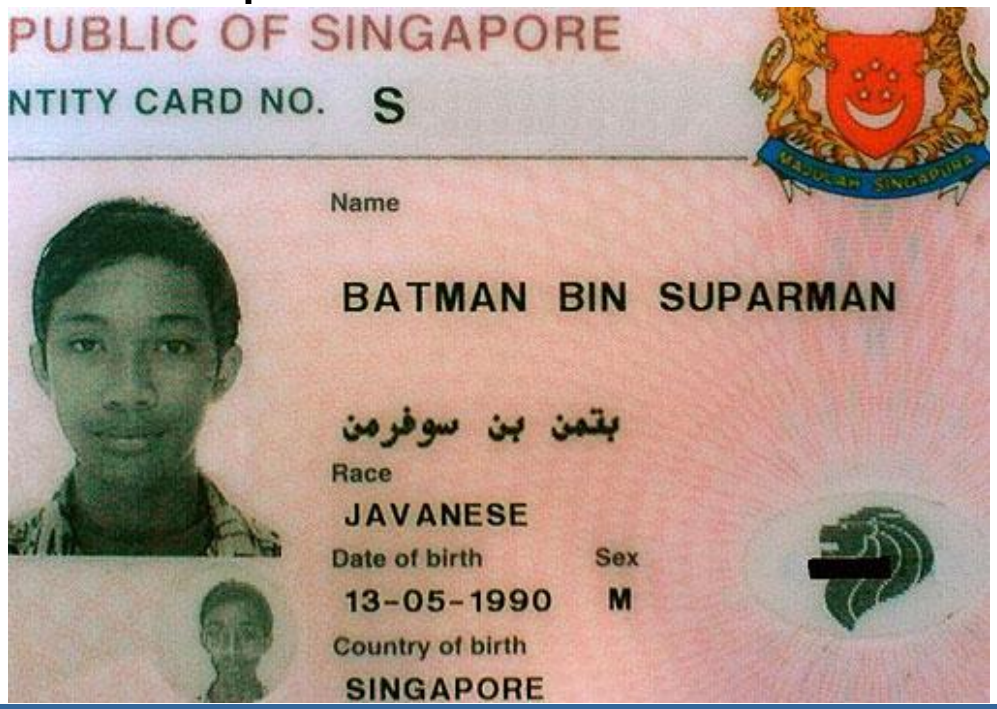
PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Implement Strong Access Control Measures

  Requirement 7: Restrict access to cardholder data by business need to know

  Requirement 8: Assign a unique ID to each person with computer access.



PCI – DSS

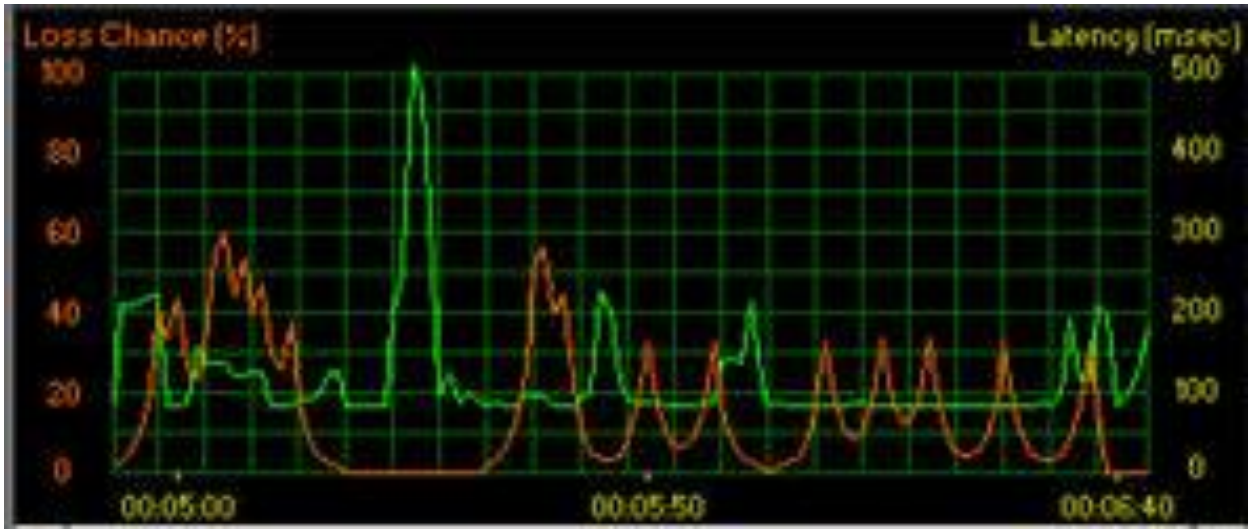
Payment Creditcard Industry Data Security Standaard

- Implement Strong Access Control Measures
  - Requirement 7: Restrict access to cardholder data by business need to know
  - Requirement 8: Assign a unique ID to each person with computer access.
  - Requirement 9: Restrict physical access to cardholder data.

PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Regularly Monitor and Test Networks

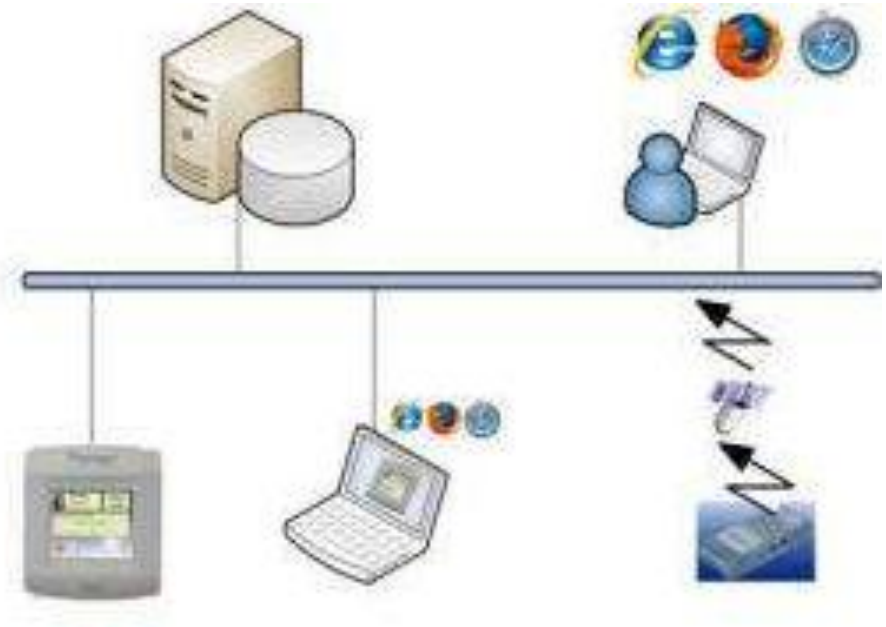


PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Regularly Monitor and Test Networks

  Requirement 10: Track and monitor all access to network resources and cardholder data.



PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Regularly Monitor and Test Networks
  - Requirement 10: Track and monitor all access to network resources and cardholder data.
  - Requirement 11: Regularly test security systems and processes.

PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Maintain an Information Security Policy

PCI – DSS

Payment Creditcard Industry Data Security Standaard

- Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for employees and contractors.

Compliancy Checklist

PCI DSS Requirements	Testing Procedures
6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release. *Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.*	**6.1.a** For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.
	6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.

Compliancy Checklist

Testing Procedures	In Place	Not in Place	Target Date/ Comments
6.1.a For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security patch list, to verify that current vendor patches are installed.			
6.1.b Examine policies related to security patch installation to verify they require installation of all critical new security patches within one month.			

The Dutch National Cybercrime Legislation

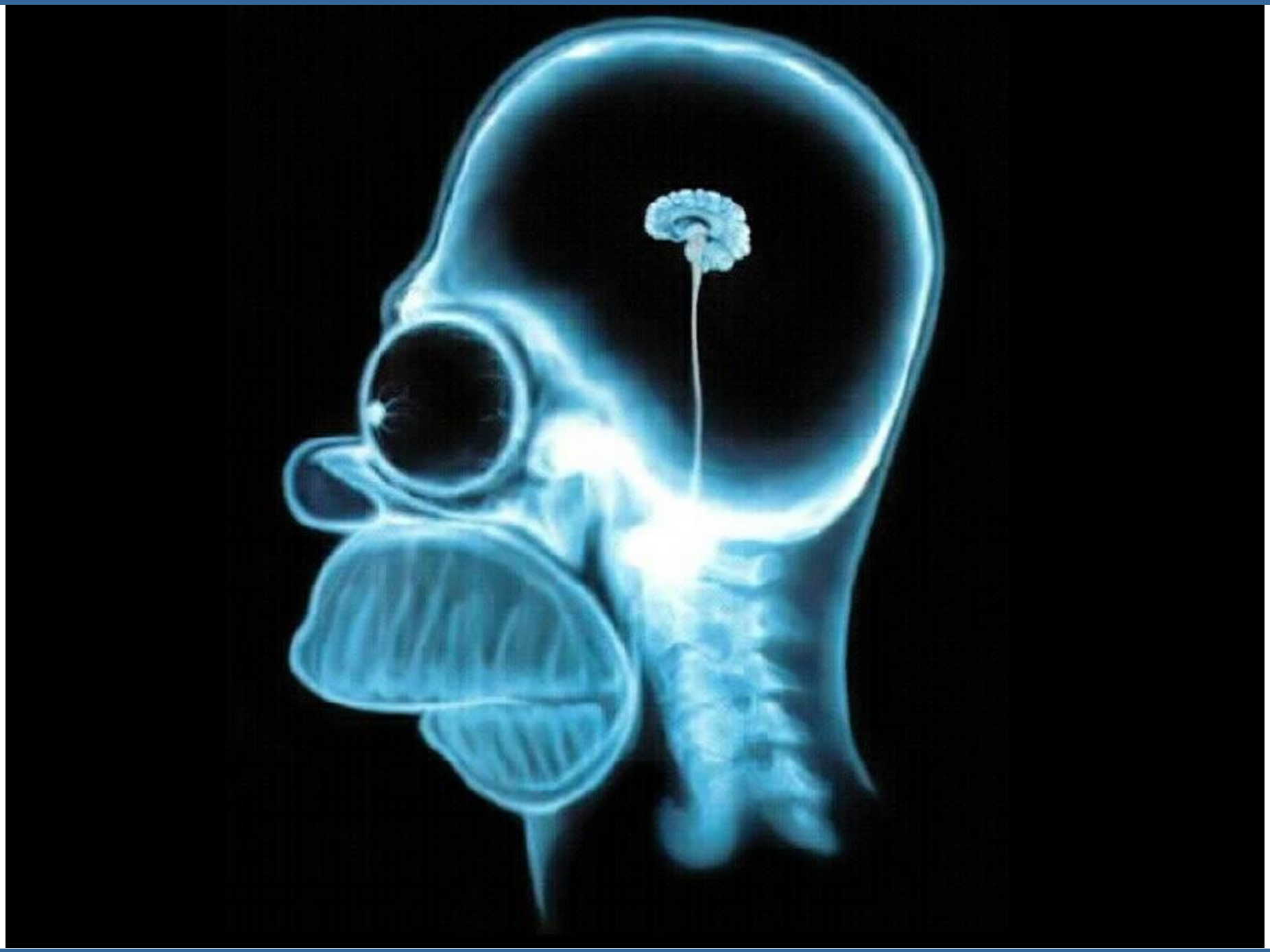
"Wet Bescherming Persoonsgegevens, "WBP"

Dutch Legislation on Personally identifiable Information (PII)

- What is Personally identifiable Information?
  - ***Information which can be used to distinguish or trace an individual's identity****, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.*2001
- PII, "personal data" is defined in EU directive 95/46/EC
  - Article 2a: *'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*

Dutch Legislation on Personally identifiable Information (PII)

- Purpose bound!
  - Whatfore the PII is stored?
  - What information is stored?
  - Where is the informaiton stored?
  - For how long the information is kept?
- For the owner of the information (the person who can be identified:
  - Can ask about the above in case of a reasonable assumption a company stores PII of him
  - Can have the PII been removed
    - if not required for other legislations as Banking
    - Goverment
    - ..etc.



That's it...

- Any Questions?

http://www.owasp.org

http://www.owasp.org/index.php/Portuguese

martin.knobloch@owasp.org

Thank you!