Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

DPbD – Storage limitation, Confidentiality and integrity & Guiding questions

Facilitating GDPR compliance for SMEs and promoting Data Protection by Design in ICT products and services (www.bydesign-project.eu)

ΑΡΧΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ

ΚΕΝΤΡΟ ΕΡΕΥΝΩΝ ΠΑΝΕΠΙΣΤΗΜΙΟΥ ΠΕΙΡΑΙΩΣ

ICT abovo Information & Communication Technologies

Το έργο χρηματοδοτήθηκε από το
Πρόγραμμα Δικαιώματα,
Ισότητα και Ιθαγένεια 2014-2020
της Ευρωπαϊκής Ένωσης

DPbD – Storage limitation

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Key design elements for storage limitation

- Deletion and anonymization – Clear internal procedures and functionalities for deletion and/or anonymization.
- Effectiveness of anonymization/deletion – Ensure that it is not possible to re-identify anonymized data or recover deleted data
- Automation – Deletion of certain personal data should be automated
- Storage criteria – Determine what data and length of storage is necessary for the purpose.
- Enforcement of retention policies – Determination of such policies and tests of whether the policies are implemented
- Justification – Justify why the period of storage is necessary for the purpose and the personal data in question (be able to disclose the rationale behind).
- Backups/logs – Determination of what personal data and length of storage is necessary for back-ups and logs.
- Data flow – Beware of the flow of personal data, and the storage of any copies thereof, and seek to limit their “temporary” storage.

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

DPbD - Bad practices in storage limitation

- Common bad practices:
  - The necessary retention period is not determined
    - The information that is given is of the type “We keep your personal data as long as necessary”
  - No automated methods for deletion – manual deletions
    - Not prohibitive, but vulnerable to human errors….
  - Anonymisation instead of deletion, but anonymisation is not effective
    - E.g. simply deleting identifiers does not yield anonymous data
  - De-activation instead of deletion
    - Data are “flagged” as deleted, but they are still there!

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

An example

- A company collects personal data where the purpose of the processing is to administer a membership of the data subject.
- The personal data shall be deleted when the membership is terminated (no legal basis for further storage of the data).
- => Internal procedure for manual deletion
  - from any devices, from backups, logs, e-mails and other relevant storage media
- To make deletion more effective, and less error-prone, the company then implements an automatic system instead, in order to delete data automatically, reliably and more regularly.

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

An example on bad anonymisation

Name	Date of birth	Sex	Zip code	Disease
Mary Adams	5/3/1995	Female	12635	Flu
John Brown	4/8/1992	Male	53715	Hepatitis
Anna Frank	10/1/1986	Female	53703	Brochitis
Tom Hill	1/2/1976	Male	12635	Broken Arm
Bob Brown	4/3/1990	Male	53706	Flu
Elen Miller	12/10/1959	Male	53700	Broken leg

Simply deleting the identifiers does not mean that the remaining data are anonymous

- Be careful on the quasi-identifiers and the relevant risks (see next seminars)

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

DPbD – Confidentiality and integrity

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

Key design elements for confidentiality and integrity

- Information security management system (ISMS) – Have an operative means of managing policies and procedures for information security.
- Risk analysis – Assess the risks against the security of personal data (several standard methodologies exist).
- Security by design – Consider security requirements as early as possible in the design
- Maintenance – Regular review and test software, hardware, systems and services, etc. to uncover vulnerabilities
- Secure transfers and storage – against unauthorized and accidental access and changes.
- Access control management – Only authorised access to strictly necessary personal data
- Pseudonymization – As a security measure to minimise risks of potential data breaches
- Backups/logs – Keep back-ups and logs that are necessary for information security, use audit trails and event monitoring as a routine security control.
- Disaster recovery/ business continuity
- Security incident response management

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

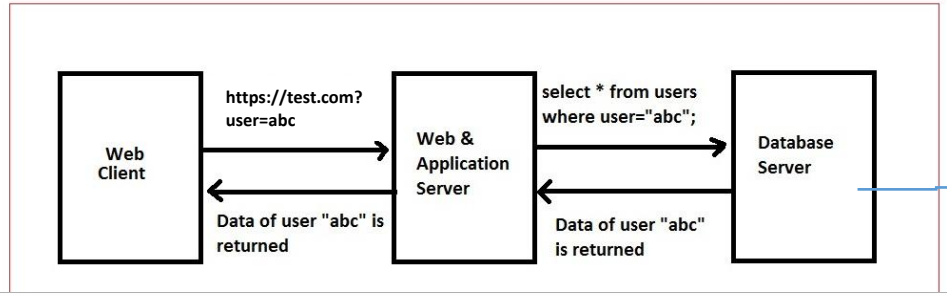
DPbD - Bad practices in confidentiality and integrity

- Common bad practices:
  - Security measures have been adopted empirically, without a systematic risk analysis
    - No proper identification of risks, which in turn means no proper choice of security measures (and not fulfillment of the accountability principle)
  - No proper access control
    - E.g. not strong authentication mechanisms or not cautious permission model for users
  - Not usage of state-of-the-art technologies (e.g. obsolete encryption)
    - E.g. Usage of the RC4 cryptographic algorithm
  - Not proper configuration of network security protocols
    - E.g. even the TLS or IPSec protocols may have vulnerabilities if they are not properly configured from the beginning
  - No regular updates/patches to critical software supporting the data processing
    - E.g. to e-commerce platforms, operating systems, other supporting software etc.

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

A bad example

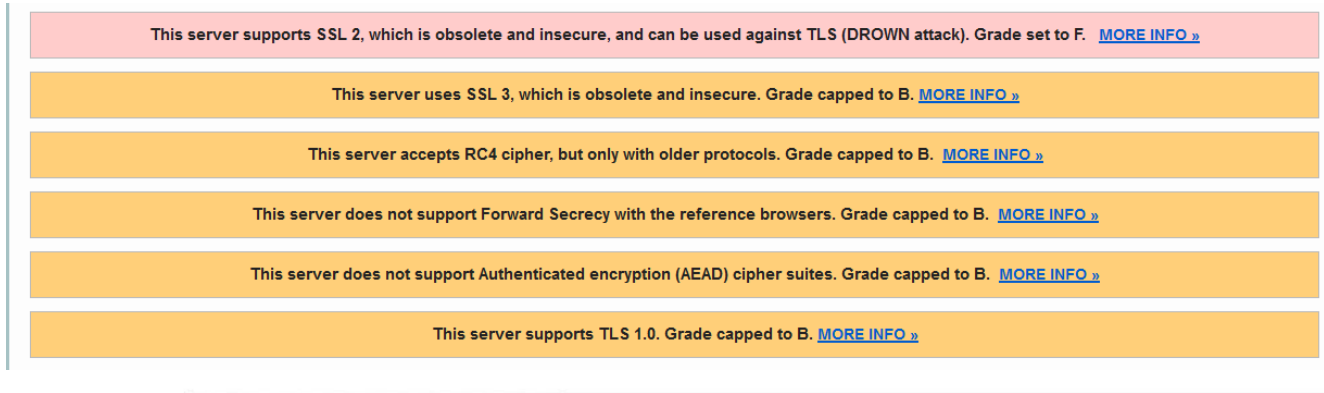
- Web form of a bookstore:
  - Use of the TLS protocol (i.e. https), version 1.2 – to protect communications with clients
    - However, protocol downgrade is possible, for allowing old browsers to connect
  - An SQL database operates “behind” the application server
    - No input sanitization; any character that the user enters in the form, passes to the SQL database
  - Passwords of the registered users are being stored in hashed form
    - Hash is mathematically irreversible, so it is being considered as a secure means to protect passwords

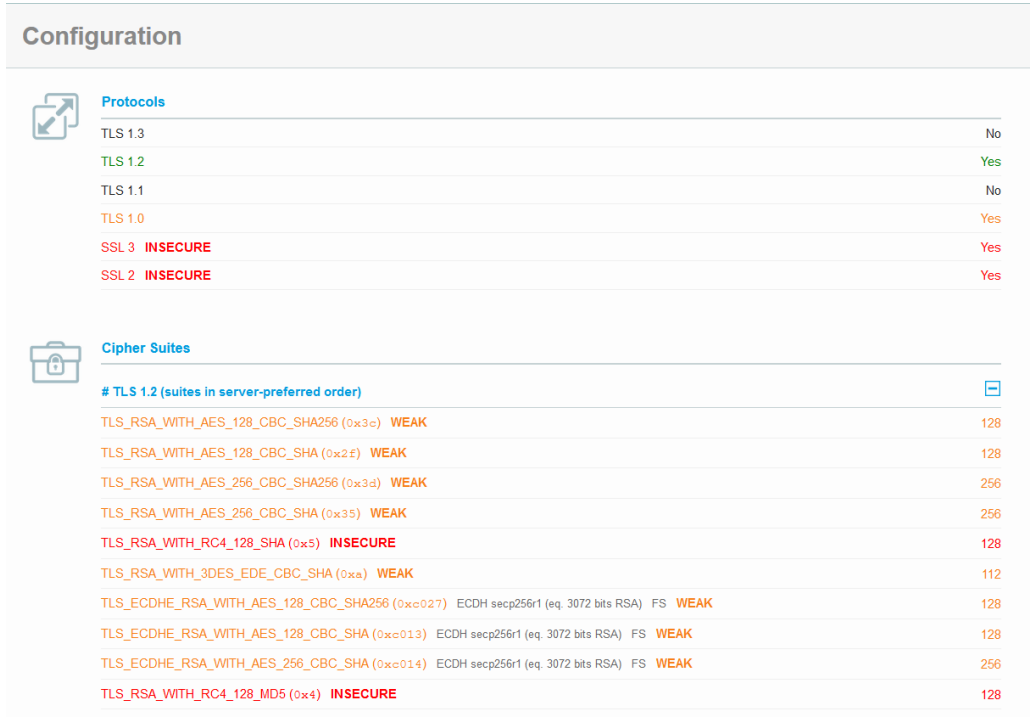


Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

A bad example (*Cont.)*

- TLS is not panacea
  - TLS 1.2 supports some weak ciphers and modes of operation, that should be avoided
  - Allowing a client to downgrade the protocol yields security issues, even for previous communications that took place with the 1.2 version! (DROWN attack)



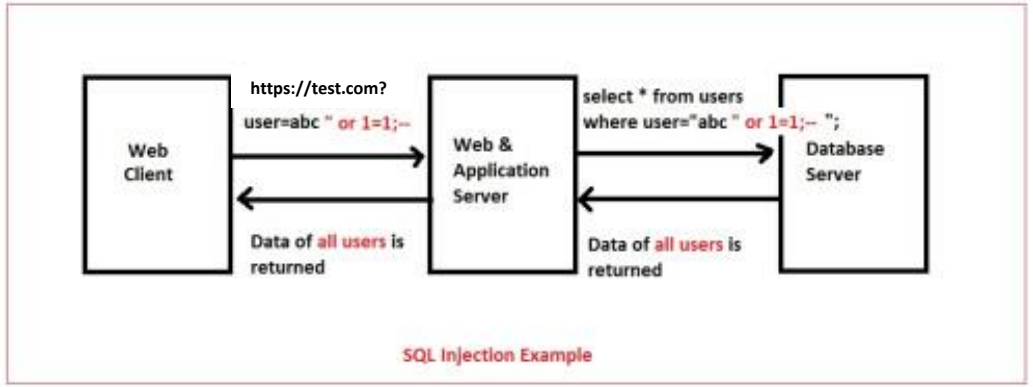


Output of a TLS scanner tool

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

A bad example (*Cont.)*

- Take care of SQL injection attacks!



- They can be avoided only if a proper design has been implemented
- A security scanner tool may detect such a vulnerability:

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

A bad example (*Cont.)*

- Hashed passwords, without salt, may be recovered
- E.g. through rainbow attacks (easily available rainbow tables, with huge number of entries)

Password	SHA-2 Hash value
123456	8D969EEF6ECAD3C29A3A629280E686CF0C3F5D5A86AFF3CA12020C923ADC6C92
abc123	6CA13D52CA70C883E0F0BB101E425A89E8624DE51DB2D2392593AF6A84118090
123456789	15E2B0D3C33891EBB0F1EF609EC419420C20E320CE94C65FBC8C3312448EB225
qwerty	65E84BE33532FB784C48129675F9EFF3A682B27168C0EA744B2CF58EE02337C5
iloveyou	E4AD93CA07ACB8D908A3AA41E920EA4F4EF4F26E7F86CF8291C5DB289780A5AE
Antetokounmpo	3AB6EAC678B05C7CFBC67E1F996D19B0F8F06C19EFDB65070B60C0BA3F6905DD
…..	

A solution would be salted hashes, where the salts are being stored in a separate place

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

An example

- A company wants to extract large quantities of personal data from a medical database containing electronic (patient) health records to a dedicated database server in the company in order to process the extracted data for quality assurance purposes.
- Since there is only one department in the company who needs to process the patient data extracts, the controller decides to restrict access to the dedicated server to employees in that department.
- Moreover, to further reduce risk, the data will be pseudonymized before they are transferred.

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

An example *(Cont.)*

- The company decides to segregate the network, and establish access controls to the server (to regulate access, protect from malware etc).
- In addition, they put up security monitoring and an intrusion detection and prevention system and isolates it from routine use
- An automated auditing system is put in place to monitor access and changes. Reporting and automated alerts are generated from this when certain events related to usage are configured.
- The company will ensure that users only have access on a “need to know” basis and with the appropriate access level.
  - Inappropriate use can be quickly and easily detected

Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

An example *(Cont.)*

- Some of the extracts have to be compared with new extracts, and therefore are required to be stored for three months.
- The company decides to put them into separate databases on the same server, and use both transparent and column-level encryption to store them.
- Keys for column data decryption are stored in dedicated security modules that can only be used by authorized personnel, but not extracted.