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

“Data Protection Principles”

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

B. Data Protection Principles

Lawfulness, Fairness and Transparency
processed lawfully, fairly and in a transparent manner in relation to the data subject

Purpose limitation
collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes

Data minimisation
adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Accuracy
accurate and, where necessary, kept up to date

Storage limitation
kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

Integrity and confidentiality
processed in a manner that ensures appropriate security of the personal data using appropriate technical or organisational measures

Accountability!
The controller shall be responsible for, and be able to demonstrate compliance with all the above

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

i. Lawfulness, fairness and transparency

'*personal data are processed lawfully, fairly and in a transparent manner in relation to the data subject*'

Fairly means transparent processing, especially when it comes to data subjects.

Data controller must inform data subjects, before the beginning of the processing, atleast for the purpose of it, the name and the address of the controller.

Unless it is provided by law, processing shouldn't be hidden or covered.

Data subjects have the right to access their data, in any case.

Apart from the obvious, this principle aims in building trust between data controller and data subject!

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

ii. Purpose limitation

'Data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes'

****further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes*

The purpose of the processing must be clearly defined *before* the beginning of the processing

- The lawfulness of processing is strongly connected with its purpose
- Processing with no clear purpose in not lawful!
- Further use of data for new purpose needs new legal base, if the new purpose in incompatible with the first one

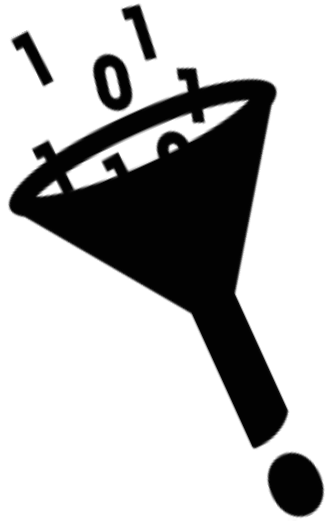
****ex.: transfer to third parties is a new purpose and new legal base is needed!*

Further use for purposes compatible with the first one is lawful and no new legal base is needed.

- GDPR doesn't define 'compatible' => ad hoc interpretation

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

iii. Data minimization



'adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed'

The data categories selected for the processing must be relevant and necessary for the fulfillment of the purpose of this processing,
Data controller must strictly limit the collection of data to those are directly linked to the specific purpose of the processing

Privacy - friendly solutions should be selected with the use of new technology, ex.:

- Non use of personal data, or
- pseudonymisation

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

iv. Accuracy

'accurate and, where necessary, kept up to date'

every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

Data controller shouldn't use data without taking measures that guarantee that data are accurate and up to date

There are cases that data must be often updated to avoid damage to the data sublects

ex. Bank institutions that check on the solvency of their customers

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

v. Storage limitations

'*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*'

***personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and security measures exist in order to safeguard the rights and freedoms of the data subject

Data subject must be informed, apart from the purpose, about the period for which the personal data will be stored

When this period ends, processing may continue only for scientific or historical research purposes or statistical purposes

***In the public sector, this period should be defined in law

vi. Integrity and Confidentiality

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

'processed in a manner that ensures appropriate security of the personal data, including protection against *unauthorised* or *unlawful* processing and against *accidental loss*, *destruction* or *damage*, **using appropriate technical or organisational measures!**

Data controller and processor have the obligation to take appropriate measures against any unauthorised processing.

The appropriate level of security is defined from:

- The **state of the art** for the security measures
- The implementation costs of the measures, and
- The level of 'sensitinity' of the data processed

Added safeguard for a safe processing is the general duty of all the persons related to the processing (controllers or processors) to ensure data privacy

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

vii. Accountability

The controller shall be responsible for, and be able to demonstrate compliance with the aforementioned principles

According to WP Art.29, in the core of accountability is the obligation of data controller to:

- implement measures that ensure the enforcement of measures taken for data protectionα
- have appropriate documents to prove and demonstrate GDPR complianc towards to HDPA and data subjects

Data controller must *at any time* be able to demonstrate to data subjects, public and supervisory authorities its compliance with the data protection rules.

****Privacy policy is one element that could show such compliance (first reference in e-privacy 2009)*