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

“Legal bases”

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

C. Legal Bases

When is processing lawful?

a. consent

The data subject has given consent to the processing of his or her personal data for one or more specific purposes

Attention to the definition of consent!

b. performance or conclusion of a contract

Processing is necessary:

-the performance of a contract to which the data subject is party, or

-in order to take steps at the request of the data subject prior to entering into a contract

c. legal obligation

Processing is necessary for compliance with a legal obligation to which the controller is subject

Apart from public sector, there also other cases where data controllers are oblidged by law to process data: ex. doctors and hospitals, employers, companies (customers data for tax purposes)

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

d. vital interest

Processing is necessary for the vital interest of data subject or of another natural person

e. public interest

Processing is necessary for the performance of a task carried out :

in the public interest or

in the exercise of official authority vested in the controller

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

Processing is necessary:

for the purposes of the *legitimate interests* pursued by the controller or a third party

except where such interests are *overridden* by the *interests* or *fundamental rights* and *freedoms* of the data subject which require protection of personal data, *in particular where the data subject is a child*.

- ✓ It's often used in private sector (ex. for financial purposes)
- ✓ Where consent cant be the legal base **(ex. video surveillance)**

Attention!

It can not be implemented in processing held by public authorities in the performance of their duties.

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

When is processing of *special categories* is lawful?

Prohibition!

Processing of special categories is prohibited.

There are still few exceptions in GDPR!

a. consent

the data subject has given explicit consent to the processing of those personal data for one or more specified purposes

Attention! The contractual relationship with the data subject is not considered as a general legal basis for the special categories

- ✓ If an airline passenger, when booking, asks the airline to offer him / her a wheelchair and a kosher meal, the airline is allowed to use this data, even though the passenger has not signed an additional clause expressly giving his or her consent to use these data which provide information about his health and religious beliefs. This action resulting from the choice of the passenger is considered as explicit consent.

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

b. Employment/ Social Security and Protection

Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of *employment* and *social security* and *social protection law* in so far as it is authorized by:

-law **provision** or

-a **collective agreement** pursuant to national law providing for appropriate safeguards for the fundamental rights and the interests of the data subject

c. vital interest

Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving **consent**

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

d. Foundations / Associations/ Non profit bodies

processing is carried out by a foundation, association or any other not-for-profit body with *a political, philosophical, religious or trade union aim,* in the course of its legitimate activities:

(a) *with appropriate **safeguards*** and

(b) on condition that the processing *relates solely to the members or to former members* of the body or to *persons who have regular contact* with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects

e. Manifestly public

processing relates to personal data which are *manifestly made public by the data subject*

f. Legal claims

processing is necessary for the *establishment*, *exercise* or *defence of legal claims* or whenever *courts are acting in their judicial capacity*

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

g. substantial public interest

Processing is necessary for substantial public interest, on the basis of Union or Member State law which:

-shall be *proportionate* to the aim pursued,

-*respect the essence* of the right to data protection and

-provide for *suitable* and *specific measures* to safeguard the fundamental rights and the interests of the data subject

h. medical data

Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law provision or pursuant to contract with a health professional

- ✓ **Further safeguards**: processing is being held by a professional or a person subject to an obligation of secrecy under
  - ✓ law provision, or
  - ✓ rules established by national competent parties (ex. professional codes of conduct)

i. Public health

Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which:

provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy

j. Research / Archiving

Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

on the basis of Union or Member State, which :

-shall be *proportionate* to the aim pursued,

-respect the *essence of the right* to data protection and

-provide for *suitable* and *specific measures* to safeguard the fundamental rights and the interests of the data subject

When is processing of data relating to *criminal offenses* and *convictions* is lawful?

Official Authority

Under the control of **Official Authority**

or

Law Provision

Processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

Any comprehensive register of criminal convictions shall be kept only under the control of official authority

- ✓ Attention!: It doesn't refer to processing by authorities competent for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security . = Directive 680/2016
- ✓ Processing by these authorities for other purposes (ex. employees data) fall within the scope of GDPR

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

CONSENT

Definition: *Consent must be a freely given, specified, informed and unambiguous indication of an individual's wishes* by which he or she, by *a statement* or by *a clear affirmative action*, signifies agreement to the processing of personal data relating to him or her

Consent is only one of the legitimate grounds for processing personal data under the GDPR.

It should only be used where an individual is offered a genuine choice to either accept or decline what is being offered. It would not be appropriate to rely on consent if, for example, the individual had no choice but to use the service or to accept the terms:

e.g. access to free wifi only if the user consents to receiving marketing materials would be unacceptable as the two things are unrelated.

There must be some form of clear affirmative action – a "positive opt in".

Consent cannot be inferred from silence, pre-ticked boxes or inactivity.

Consent must be as easily revoked as it is given, and therefore clear processes should be in place for individuals to withdraw consent.

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

Components of *valid* consent

Freely given

Free means real choice for the data subject

- Where there is a clear inequality between the data subject and the controller consent cannot be considered as "freely given"
  - In cases, where the controller is public authority consent is really difficult to be considered as free
  - The same applies Blanket consent for a number of processing activities is not valid, there needs to be consent processes for each separate element of data processing
  - in the labour sector
- The data subject may always have the right to object or withdraw his/her consent without suffering any detriment

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

Specified

1. **Purpose determination**

2. **Separate consent for each purpose**
   - General purposes should be avoided
   - It may cover more than one processings as long as they have the main purpose
3. **Separate and clear information on processing before consent**

Data controllers should provide data subjects with information on the categories of data processed for each purpose, in order for the data subjects to be able to know the effects or risks of the processing

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

informed

- **Information** provided should be at least the following:
  - Controller's identity
  - Purpose of each processing for which consent is needed
  - Categories of data collected and processed
  - Existence of the right to withdraw
  - Use of automated decision making, including profiling
  - In case there is a transfer to third countries, information on the risks
- **Ways/Methods** of providing information
  - GDPR doesn't give specific direction, defines though that it should be clear and in simple words
  - Language and text comprehensible by an average citizen .no legal text or terms

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

affirmative declaration of consent

- GDPR requires declaration or affirmative action of the data subject
  - Not acceptance after simple information with no further action
  - Pre-ticked or opt-out boxes are not considered as valid consent
  - Any means may be used for reception of consent as long as controller can prove that consent is given
    - Ideally in written form!
    - Recording if appropriate prior information has been provided
- By electronic means…
  - Controllers can create their own systems as long as they are based on GDPR rules and principles, ex:
    - Swipe, mobile rotation in 8 etc.
    - A simple scroll in the text doesn't meet the requirement

Child's consent

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

Special child protection in relation to the offer of information society services directly to a child

Consent is valid ONLY if it is given or authorised by the holder of parental responsibility over the child (parent or guardian)

Especially in the use of personal data for the purpose of marketing or creating a personality profile or user profile
The consent of a parent or guardian should not be required in the case of prevention services or counseling offered directly to a child.

GDPR set an age limitation: *Under 13 =not valid consent =unlawful processing*
Over 16 =valid =lawful processing

In Greece, a child may give its own, valid consent, when she/he is over 15 years old.

Data controller must verify that consent is given or authorized by the parent or the guardian.

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

Things to do now if you are relying on consent to process data:

Identify where you are relying on consent to process personal data / special categories data:

- Review *how* you collect the consent (information sheets, data collection notices, forms etc.)
- Make sure you are collecting *a freely given, specified, informed* and *unambiguous indication* of an individual's wishes (what are you telling them?);
- Can you offer individuals the opportunity to *consent to certain areas of the processing* and utilise a "positive opt in" – e.g. a tick box process? *This could be useful for research projects*.
- Consider *how individuals can revoke* their consent? Is it *clear* from your documentation / website? It needs to be as clear as the process you utilised to collect the consent, and individuals should be able to notify you through the same medium.
- *What do you do with consent* already collected?