



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

# “Data subjects’ rights”

*Facilitating GDPR compliance for SMEs and promoting Data Protection by  
Design in ICT products and services*

*([www.bydesign-project.eu](http://www.bydesign-project.eu))*





## D. Data Subject Rights

Transparent communication and modalities (art. 12).

- (1) Right to be informed (art. 13, 14).
- (2) Right of access (art. 15).
- (3) Right of rectification (art. 16).
- (4) Right to erasure/ right «to be forgotten» (art. 17).
- (5) Right to restriction of processing (art. 18).
- (6) Right to data portability (art. 20)
- (7) Right to object (art. 21).
- (8) Right to non automated decision making, including profiling (art. 22).



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



# Transparent information, communication and modalities for the exercise of the rights



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

Information and communication should be provided in the following cases:

- before / during processing,
- exercise of rights and
- data breach.
- Concise, transparent, intelligible and easily accessible form.
- **Way of information:** in *writing* or by other means, inter alia, *by electronic means, where appropriate*.
- **Orally, when requested by the data subject:** provided that the identity of the data subject is proven by other means.
- Information shall be provided **free of charge** (a *reasonable fee* may be charged, if the requests are manifestly unfounded or excessive, in particular because of their repetitive character,).





- **Deadline for the controller to provide information:**
  - without undue delay and in any event within **one (1) month** of receipt of the request.
  - Extension of period by **two (2) further months** taking into account the **complexity** and **number** of the requests.
  - Data subject should be in any case informed of any extension and the reasons for it within **one (1) month**.
- **No action taken by the controller:**
  - the controller shall inform the data subject **without delay** and **at the latest within one (1) month** of receipt of the request:
  - of the **reasons** for not taking action and
  - on the possibility of lodging a **complaint** with a supervisory authority and seeking a judicial remedy.

## 1a. Right to be informed when data *are being obtained* from the data subject



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



- **Identity/Contact details** of data controller.
- **Contact details** of Data Protection Officer (DPO).
- **Purpose** of processing – **legal base**.
- **Legitimate interest** of data controller or third party.
- **Recipients** or categories of recipients.
- **Transfer** to third country or international organization.
- **Storage period** or criteria of such storage.
- Existence of the **right** to request access to or rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability .
- Right to **withdraw consent**.
- Right to **lodge complaint** with a supervisory authority.
- Whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the **possible consequences** of failure to provide such data.
- Existence of automated decision-making, including profiling.

**Right to Know. Right Now!**

## 1b. Right to be informed when data *have not been obtained* from the data subject



- **Further** to the previous ones:
  - **Categories** of data
  - From which **source** the personal data originate, and if applicable, whether it came from **publicly accessible sources**.
- **When is the data subject is informed?**
  - within a **reasonable period** after obtaining the personal data,
  - but at the **latest within one (1) month**, having regard to the specific circumstances in which the personal data are processed
  - at the latest at the time of the **first communication** to that data subject, if the personal data are to be used for communication with the data subject,.
  - at the latest **when the personal data are first disclosed**, if a disclosure to another recipient is envisaged.



## Exception from the right to be informed when data are obtained from other sources



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

- If data subject already has the information.
- the provision of such information proves
  - **impossible** (ex. **there are no contact details of data subject**) or information would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,
  - in so far as the information is likely to render impossible or seriously impair the achievement of the objectives of that processing. (ex: money laundry)
  - data controller makes information publicly available
- obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject and which provides appropriate measures to protect the data subject's legitimate interests (ex. **tax legislation**)
- where the personal data must remain *confidential* subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy (ex. **receipt of medical history of relative**).



## 2. Right of access

- The data subject shall have the right:
  - a. to obtain from the controller confirmation of processing and, where that is the case, access to the personal data and specific information (*see below*), and
  - b. A copy of his/her data
- **No justification** is required.
- **Verification by any means** of data subject's identity by data controller.
- Providing **remote access to a secure system**.
- **Provision of a copy** of the data also in electronic form (free of charge and for additional copies a reasonable fee for administrative expenses)
- **Facilitating the subject** to exercise the right of access.
- Possibility of electronic submission of requests especially for data in electronic form.
- **Examples:**
  - *Online form on a website.*
  - *Printed form at reception point*





## ...*access to what information?*

- **Purpose of processing.**
- Categories of **data**.
- **Recipients or categories of recipients** to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations.
- the envisaged **period** for which the personal data will be stored, or, if not possible, the criteria used to determine that period.
- Existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing.
- Existence of the right to lodge a complaint with a supervisory authority.
- Where the personal data are not collected from the data subject, any available information as to their source.
- The existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.



### 3. Right to rectification



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

- The data subject has the right :
  - **to obtain Rectification of inaccurate personal data,**
  - to have **incomplete personal data completed,** including by means of providing a supplementary statement.



*Examples: the indication that someone is married while he is not, the non-updating of the TIREZIA database.*

- It's up to the data subject to determine which data need correction ex. wrong name.



## 4. Right to erasure /right 'to be forgotten'



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

### **Only when:**

- Data are **no longer necessary** for the purpose of processing.
- **Withdrawal of consent** and of any other legal base.
- The data subject **objects** to the processing and there are no overriding legitimate grounds for the processing.
- **Unlawful** processing.
- Compliance of data controller with legal obligation for erasure.
- Personal data have been collected in relation to the offer of information society services directly to the **child**.





# Exceptions!



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

## *When processing is necessary for:*

- exercising the right of freedom of expression and information,
- compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller,
- reasons of public interest in the area of public health,
- archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,
- the establishment, exercise or defence of legal claims.



## 5. Right to restriction of processing

### **Only where:**

- the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data,
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead,
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims,
- the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

### **Possible ways:**

- *Temporary move of data to another system.*
- *Remove accessibility of selected data by users.*
- *Temporarily remove data from a web page.*





## 6. Right to portability



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



The data subject shall have the right to:

- a) **receive** the personal data concerning him or her, **which he or she *has provided to a controller\****, in a structured, commonly used and machine-readable format\*\*, and
- b) have the right to **transmit** those data to another controller **without hindrance** from the controller to which the personal data have been provided

**Only where:**

- the processing is based on **consent** or on a **contract**, and
- the processing is carried out by automated means
- the processing does not adversely affect rights and freedoms of others

*\*consciously - actively provided / observed activity, ex. Search history. NO: deduced / produced data, ex. Health assessment, profile.*

*\*\* security measures / costs taken into account*



## 7. Right to object



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

Only where the legal base of the processing is:

- the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- 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.*

\*\*\* Where the data subject objects to processing for **direct marketing purposes**, the personal data shall no longer be processed for such purposes

- **Exception!**

When processing is necessary for the performance of a task carried out in the public interest and the data are processed *for scientific or historical research purposes or statistical purposes.*

Results: END of processing!



## 8. Right to non-automated decision making



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

- Data subject's right to:
  - not to be subject to a decision based solely on automated processing, including profiling,
  - which produces legal effects concerning him or her or similarly significantly affects him or her (*ex. automatic denial of an online credit application*)
- It doesn't apply when the decision:
  - (a) is necessary for the entering into, or performance of, a contract between the data subject and a data controller,
  - (b) ) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests,
  - (c) is based on the data subject's explicit consent.
- In cases (a) and (c) the controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.

