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

"Key GDPR Definitions"

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

(www.bydesign-project.eu)

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

A. *What is data protection?*

Data protection is the fair and proper use of information about people.

It's part of the fundamental *right to privacy* – but on a more practical level.

It's really about building trust between people and organisations. It's about treating people fairly and openly, recognising their right to have control over their own identity and their interactions with others, and striking a balance with the wider interests of society. It's also about removing unnecessary barriers to trade and co-operation. It exists in part because of international treaties for common standards that enable the free flow of data across borders.

Data protection is essential to innovation. Good practice in data protection is vital to ensure public trust in, engagement with and support for innovative uses of data in both the public and private sectors.

The greek data protection regime is set out in the Act 4624/2019 and GDPR.

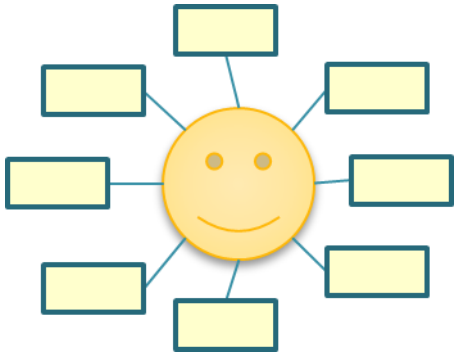
GDPR article 4: DEFINITIONS

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

1) ‘personal data’
2) ‘processing’
3) ‘restriction of processing’
4) ‘profiling’
5) ‘pseudonymisation’
6) ‘filing system’
7) ‘controller’
8) ‘processor’
9) ‘recipient’
10) ‘third party’
11) ‘consent’
12) ‘data breach’
13) ‘genetic data’
14) ‘biometric data
15) ‘data concerning health’
16) ‘main establishment’
17) ‘representative’
18) ‘enterprise’
19) ‘group of undertakings’
20) ‘binding corporate rules’
21) ‘supervisory authority’
22) ‘supervisory authority concerned’
23) ‘cross-border processing’
24) ‘relevant and reasoned objection’
25) ‘information society service’
26) ‘international organisation’

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

PERSONAL DATA



Ex. personal data: name and surname, a home address, an email address such as name.surname@company.com, an identification card number, location data (for example the location data function on a mobile phone), an Internet Protocol (IP) address, a cookie ID, the advertising identifier of your phone, data held by a hospital or doctor, which could be a symbol that uniquely identifies a person

Ex. non personal data: a company registration number, an email address such as info@company.com , anonymised data

*any information relating to an identified or identifiable natural person ('**data subject**'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*

(example: document including initials uploaded on 'https://diavgeia.gov.gr')

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

Few more words…

Personal data means information about a particular *living individual*. This might be anyone, including a customer, client, employee, partner, member, supporter, business contact, public official or member of the public. It doesn't need to be 'private' information – even information which is public knowledge or is about someone's professional life can be personal data.

Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data that has been *de-identified*, *encrypted* or *pseudonymised* but can be used to reidentify a person remains personal data and falls within the scope of the GDPR. Personal data that has been rendered *anonymous* in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

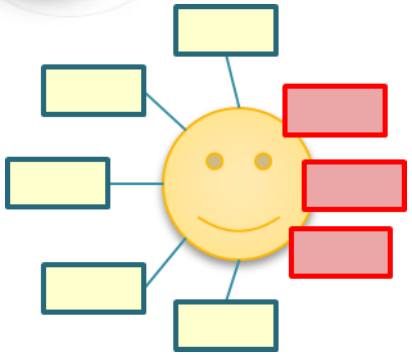
The GDPR protects personal data regardless of the technology used for processing that data – it's technology neutral and applies to both automated and manual processing, provided the data is organised in accordance with pre-defined criteria (for example alphabetical order).

It also doesn't matter how the data is stored – in an IT system, through video surveillance, or on paper;

In all cases, personal data is subject to the protection requirements set out in the GDPR.

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

Special categories of data



data revealing: *racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*

- «**genetic data**»:data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question,
- «**biometric data**»:data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person
  - ex. facial images or dactyloscopic data
- «**health data**»:data related to the physical or mental health of a natural person
- Separate «special» category: **criminal convictions and offenses**

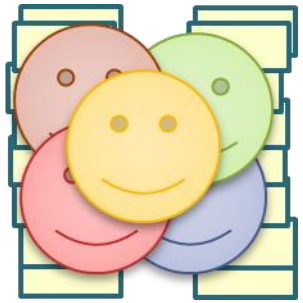
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

What does 'processing' mean?

Almost anything you do with data counts as processing!

GDPR: "Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means"

- *collection,*
- *recording,*
- *organisation,*
- *structuring,*
- *storage,*
- *adaptation or alteration,*
- *retrieval,*
- *consultation,*
- *use,*
- *disclosure by transmission,*
- *dissemination or otherwise making available,*
- *alignment or combination,*
- *restriction,*
- *erasure or destruction*



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

Examples of processing :

- staff management and payroll administration
- access to/consultation of a contacts database containing personal data
- sending promotional emails
- shredding documents containing personal data
- posting/putting a photo of a person on a website
- storing IP addresses or MAC addresses
- video recording (CCTV)

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

DATA SUBJECT

'personal data' means any information relating to *an identified or identifiable natural person* …'

This is the technical term for the individual whom particular personal data is about.

What are identifiers and related factors?

An individual is 'identified' or 'identifiable' if you can distinguish them from other individuals.

A **name** is perhaps the most common means of identifying someone.

However whether any potential identifier actually identifies an individual depends on the context.

A combination of identifiers may be needed to identify an individual.

***GDPR provides a non-exhaustive list of identifiers, including: name; identification number; location data; and an online identifier. 'Online identifiers' includes IP addresses and cookie identifiers which may be personal data. Other factors can identify an individual.

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

"…relates to…"

What is the meaning of 'relates to'?

Information must 'relate to' **the identifiable individual** to be personal data.

Not simply identifying a natural person – it must concern him/her in some way.

***To decide whether or not data relates to an individual, you may need to consider:

-the *content* of the data – is it directly about the individual or their activities?;

-the *purpose* you will process the data for; and

-the *results* of or *effects* on the individual from processing the data.

Data can reference an identifiable individual and not be personal data about that individual, as the information does not relate to them.

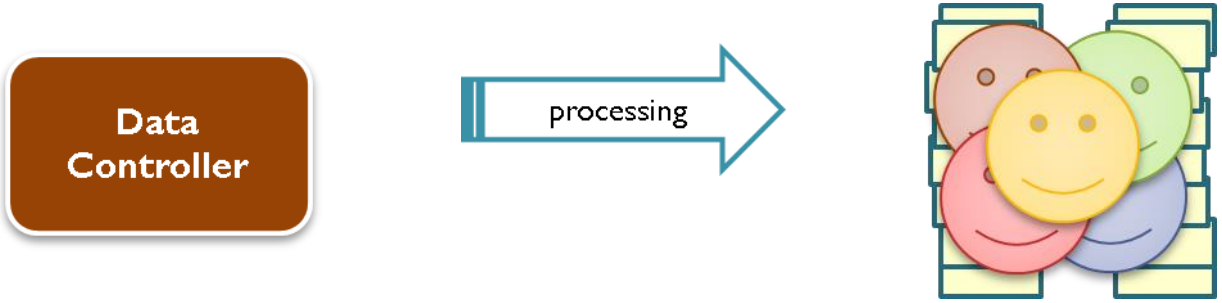
There are circumstances where it is difficult to determine whether data is personal data.

Good practice: you should treat the information with care, ensure that you have a clear reason for processing the data and, in particular, ensure you hold and dispose of it securely.

Inaccurate information may still be personal data if it relates to an identifiable individual.

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

Data Controller



'Any natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the *purposes* and *means* of the processing of personal data'

ATTENTION!:where the purposes and means of such processing are determined by Union or Member State law, *the **controller** or the specific **criteria for its nomination** may be provided for by Union or Member State law*

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

What is namely a ‘data controller’?

A controller is the person that **decides how and why to collect and use the data**. This will usually be an organisation, but can be an individual (*eg. a sole trader, a doctor, a lawyer etc*).

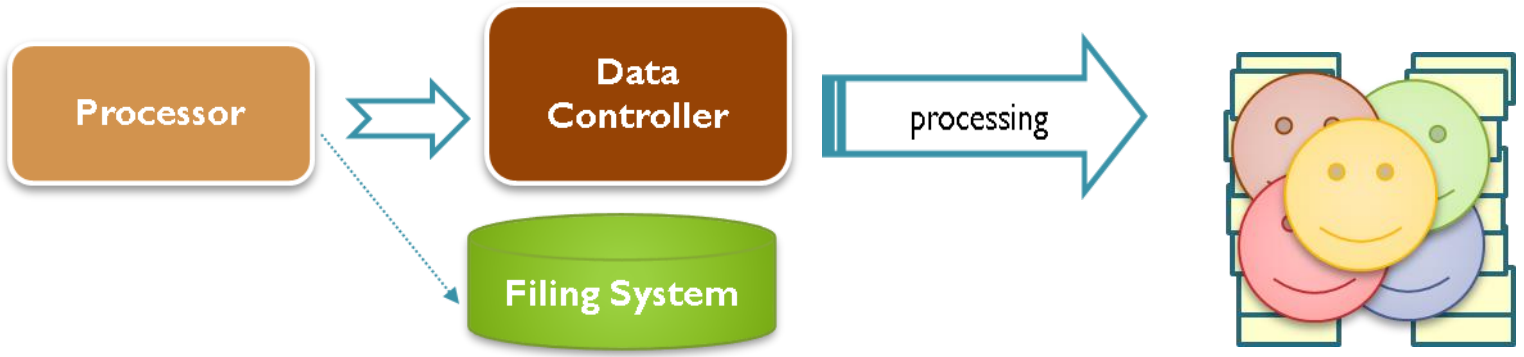
If you are an employee acting on behalf of your employer, the employer would be the controller.

The controller must make sure that the processing of that data complies

with data protection law.

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

Processor



"*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*"…and in accordance with their instructions

****NOT an employee!!!*

***Processors have some direct legal obligations, but these are more limited than the controller's obligations

- ✓ Typical case of processor is the «subcontractors», as long as they process personal data.
- ✓ In public sector, processors may be other public authorities, ex.: Taxisnet, G-Cloud, IDIKA.

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

Example of CONTROLLER - PROCESSOR

Q. Organisation A provides payroll processing services to corporate customers. Organisation A provides those services to its customers in accordance with each customer's instructions. Organisation A also uses those data to perform benchmarking analysis, so that it can sell further services allowing customers to compare their payroll data to industry averages.

Does Organisation A fall within the definition of a "controller" or a "processor"?

A. Depending on the facts, the same entity can be a controller in respect of some processing activities and a processor in respect of other processing activities. In this example, Organisation A is a processor in respect of the payroll processing services it provides directly to its customers, and a controller in respect of the benchmarking services, as it is processing personal data to create benchmarks for its own purposes.

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

JOINT CONTROLLERS

"two or more controllers jointly determine the purposes and means of processing"

Joint controllership exists with regard to a specific processing activity when different parties determine jointly the purpose and means of this processing activity. They must in a transparent manner *determine* their respective responsibilities for compliance with the obligations under GDPR, in particular as regards the exercising of the rights of the data subject by means of an *arrangement* between them *unless*, the respective responsibilities of the controllers are determined by Union or Member State *law* to which the controllers are subject.

Therefore, assessing the existence of joint controllers requires examining whether the determination of purposes and means that characterize a controller are decided by more than one party.

"Jointly" must be interpreted as meaning "together with" or "not alone", in different forms and combinations.

Not all processing involving several entities give rise to joint controllership. The overarching criterion for joint controllership to exist is the joint participation of two or more entities in the determination of the purposes and means of a processing

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

Examples of JOINT CONTROLLERS

1. A **travel agency** sends personal data of its customers to the **airline** and a **chain of hotels**, with a view to making reservations for a travel package.

The airline and the hotel confirm the availability of the seats and rooms requested. The travel agency issues the travel documents and vouchers for its customers. Each of the actors processes the data for carrying out their own activities and using their own means. In this case, the **travel agency, the airline** and **the hotel** are three different data controllers processing the data for their own and separate purposes and there is no joint controllership.

2. The **travel agency**, the **hotel chain** and the **airline** then decide to participate jointly in setting up an internet-based common platform for the common purpose of providing package travel deals. They agree on the essential means to be used, such as which data will be stored, how reservations will be allocated and confirmed, and who can have access to the information stored. Furthermore, they decide to share the data of their customers in order to carry out joint marketing actions. In this case, the travel agency, the airline and the hotel chain, jointly determine why and how personal data of their respective customers are processed and will therefore be joint controllers with regard to the processing operations relating to the common internet-based booking platform and the joint marketing actions. However, each of them would still retain sole control with regard to other processing activities outside the internet-based common platform.

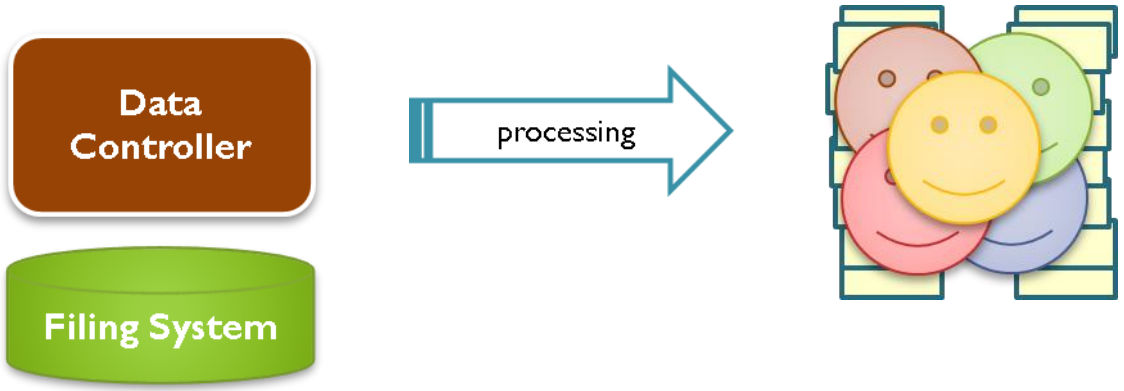
Το έργο χρηματοδοτήθηκε από το Πρόγραμμα Δικαιώματα, Ισότητα και Ιθαγένεια 2014-2020 της Ευρωπαϊκής Ένωσης

3. **Several research institutes** decide to participate in a specific joint research project and to use to that end the **existing platform** of one of the institutes involved in the project.

Each institute feeds personal data it already holds into the platform for the purpose of the joint research and uses the data provided by others through the platform for carrying out the research. In this case, all institutes qualify as joint controllers for the personal data processing that is done by storing and disclosing information from this platform since they have decided together the purpose of the processing and the means to be used (the existing platform). Each of the institutes however is a separate controller for any other processing that may be carried out outside the platform for their respective purposes.

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

Filing System

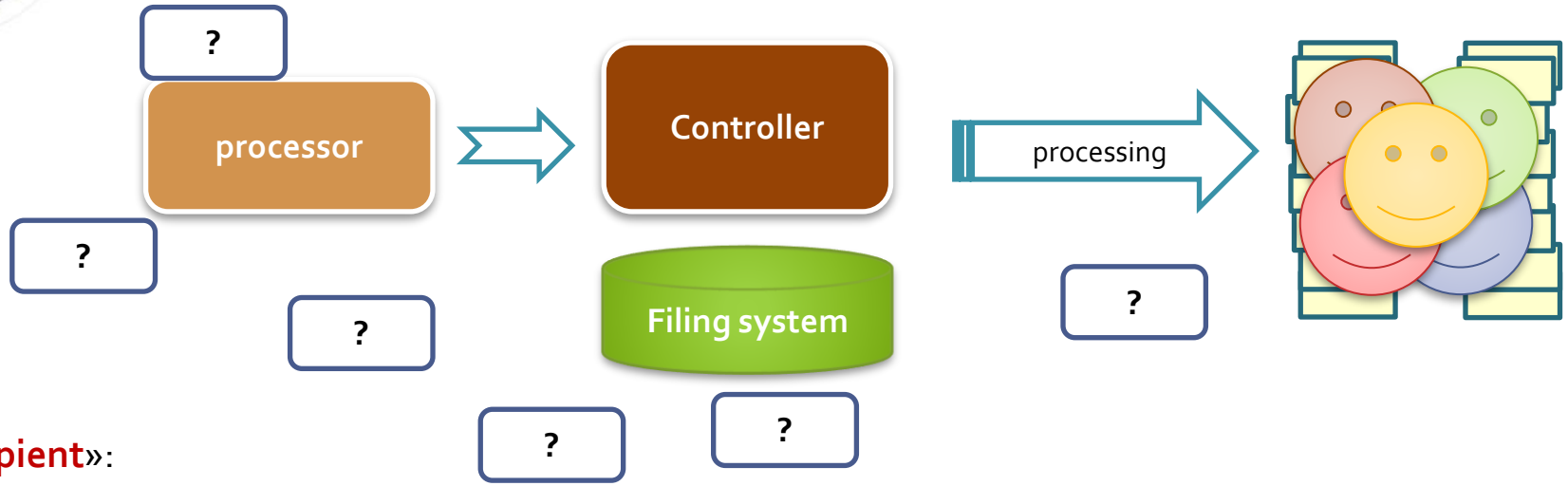


«**filing System**»:

- any structured set of personal data
- accessible according to specific criteria,
- whether centralised, decentralised or dispersed on a functional or geographical basis

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

Other parties - Definitions



«**Recipient**»:

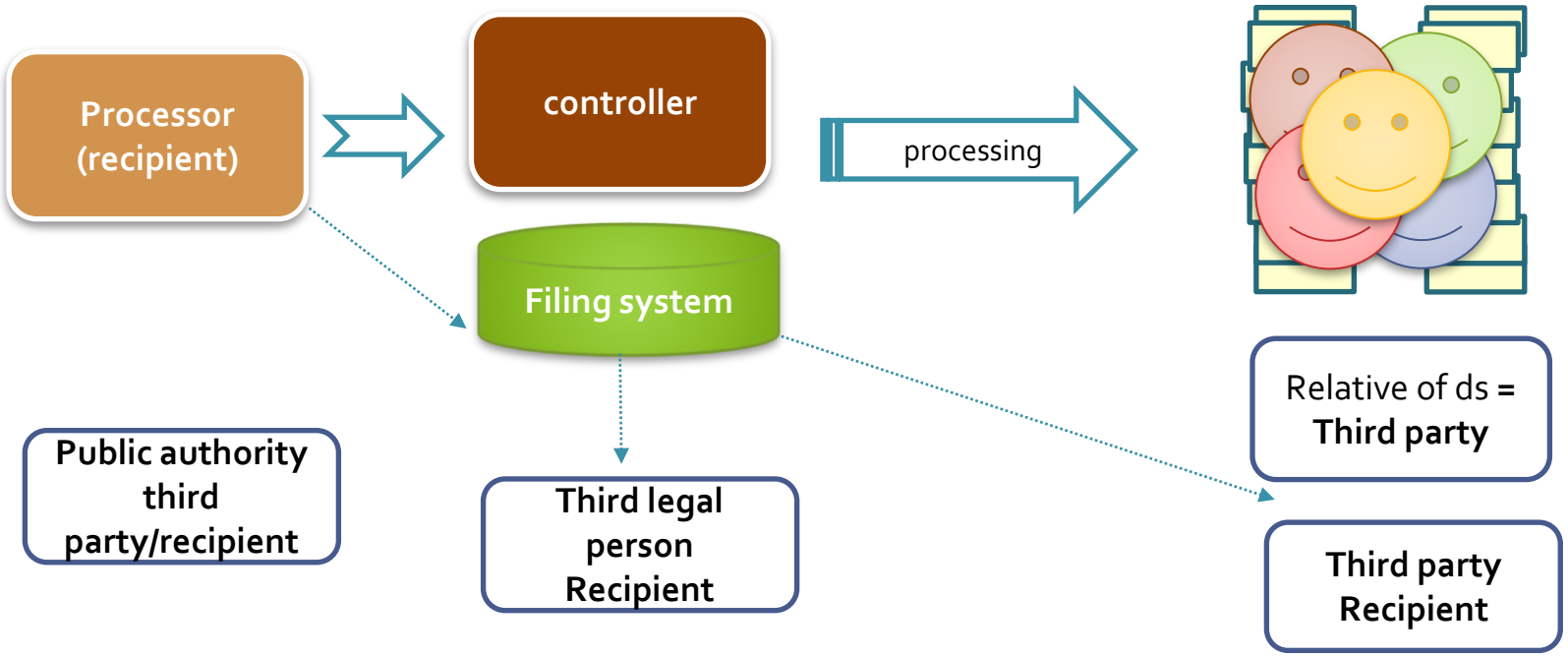
- a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.
- *However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients;*

«**Third Party**»: any natural or legal person, public authority, agency or body, except for:

- data subject,
- processor and
- Persons who, under the direct authority of the controller or processor, are authorised to process personal data

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

Recipients and third parties

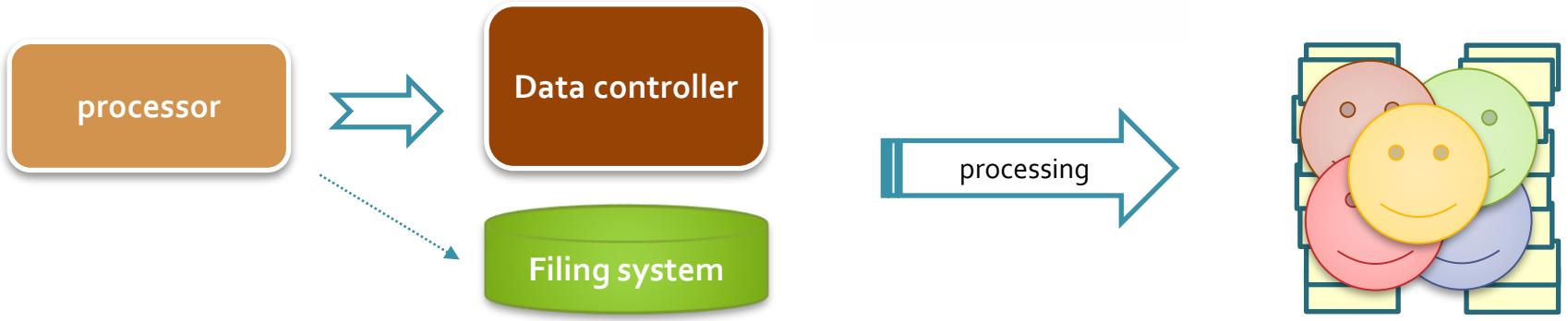


- ✓ Processors are «**recipients**», not «**third parties**».
- ✓ The exemption of public audit authorities applies to individual cases, in order to facilitate their work
  - ✓ These authorities though are data controllers for the data they process for their purposes

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

...last but not least

HELLENIC DATA PROTECTION AUTHORITY



«**Supervisory Authority**»:

- Member states shall determine the full status of operation and independence
- HDPA is enshrined in Greek Constitution (art. 9A) and its status is governed by Act. 3051/2002

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

Few more words…

DPAs are independent public authorities that:

- supervise the application of the data protection law, through *investigative* and *corrective powers*,.
- provide *expert advice* on data protection issues and
- handle complaints lodged against violations of the GDPR and the relevant national laws.
- there is, at least, one in each EU Member State.

***The main contact point for issues on data protection is the DPA in the EU Member State where your company/organisation is based. However, if your company/organisation processes data in different EU Member States or is part of a group of companies established in different EU Member States, that main contact point may be a DPA in another EU Member State.