Centre for European Constitutional Law
Themistokles and Dimitris Tsatsos Foundation

International Union of Judicial Officers
Union internationale des huissiers de justice

Creating Privacy Awareness in Civil Enforcement

101090018 — PACE — JUST-2022-JTRA

Practical Guide for data protection in civil enforcement

Deliverable 2.2

Co-funded by the European Union

CENTRE FOR EUROPEAN CONSTITUTIONAL LAW
THEMISTOKLES AND DIMITRIS TSATSOS FOUNDATION

International Union of Judicial Officers
Union internationale des huissiers de justice

Deliverable	2.2
Coordination:	Dr. Maria Mousmouti, Executive Director, CECL
Main Author:	Panagiota Siamandoura, Lawyer, Certified DPO Executive, GDPR GREECE PC Marianna Ntaliakoura, Lawyer, Certified DPO Executive, GDPR GREECE PC
Contributor:	Jos Uitdehaag (UIHJ)
Input and feedback:	Zlaty Mihailoff (UIHJ) George A. Grigoris (Judicial Officer, Appeals Court of Athens, Greece) Dragomir Yordanov (Director of the Enforcement Training Centre, Kosovo; former minister of justice of Bulgaria; former director of the Bulgarian Judicial Academy)

Disclaimer: This guide includes a simple presentation of the framework for the protection of personal data, as applied in the exercise of the duties of the enforcement agents. For this purpose, it includes some simplified concepts and examples that do not constitute legal advice. In no case should the reader consider that all cases are included in this guide and can be treated in the exact same way. The reader should therefore decide on a case-by-case basis, based on the specific data per case and consult experts if necessary.

Table of contents

Co-funded by the European Union

Co-funded by the European Union

ABBREVIATIONS

DPA	Data Protection - Authority in each Member State
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
Enforcement agent	Generic term which covers a wide variety of persons (e.g. enforcement officer, enforcer, huissier de justice, enforcement judge etc) who have in common an authorization by the state to carry out the enforcement process
Enforcement Law	Generic term covering the legislation regarding the organization of enforcement and enforcement proceedings in the respective Member States
GDPR	Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (repealing directive 95/46/EC (General Data Protection Regulation)

Co-funded by
the European Union

1. EXECUTIVE SUMMARY

This Guide aims to underline the basic provisions and principles that every Data Controller and Data Processor should be aware of, in order to protect any personal data in the context of their everyday tasks and duties. The Guide describes the basic definitions concerning personal data, as well as the basic principles and rules provided by the law, through simple examples. In addition, different cases of data breaches are being mentioned and simple measures of safety are being suggested. The Guide is addressed to enforcement agents from different countries, it thus focuses on the general provisions of the Regulation (EU) 2016/679 which are applicable despite the presence – or even the absence- of more specific provisions in each state.

2. INTRODUCTION

2.1 Purpose

This guide is addressed primarily to judicial officers and aims to inform them of the basic principles and rules while processing personal data in the context of their duties, regardless of the more specific legislative and regulatory framework per state.

These general obligations are provided by the REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR), which is directly applicable in all Member States[1].

2.2 Territorial scope

This Guide concerns not only judicial officers from EU member states but also from other states under conditions.

The GDPR applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the European Union, regardless of whether the processing takes place in the European Union or not.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1, available at https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679

Co-funded by the European Union

In specific, the GDPR applies to the processing of personal data of data subjects who are in the European Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behavior as far as their behavior takes place within the Union.

In addition, it applies to the processing of personal data by a controller not established in the European Union, but in a place where Member State law applies by virtue of public international law.

2.3 Basic GDPR definitions

For the purposes of this Guide:

(1) '**File'** the collection of data and documentation [e.g., of the client (creditor) and debtor] that relates to a particular case. The data can be written, tangible data or electronic data.

(2) **'personal data'** means any information relating to a natural person that is or can be identified (the data subject).

EXAMPLES of personal data: name, surname, tax registration number, date of birth, address, phone number, email address, financial status, bank account, property, etc.

So, any information related to a person may be defined as personal data.

(3) 'Profiling': any form of automated processing of personal data that evaluates certain personal aspects of a natural person on the basis of personal data, in particular with the aim of analyzing or predicting his professional performance, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

(4) 'Consent of the data subject' any free, specific, informed and unambiguous expression of will by which the data subject, by means of a statement or an unambiguous active act, accepts the processing of personal data concerning him or her.

(5) **'processing'** means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure erasure, etc.

So, any use of personal data is considered as processing.

(6) **'controller'** means the 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;

Co-funded by the European Union

So, Data Controller is a person or an entity that collects personal data and processes them in the context of their everyday routine (e.g. an employer processes the employee's data).

(7) **'processor'** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

So, Data Processor is a person or an entity who processes personal data on behalf of the controller and under mandates (e.g. an independent person or entity who provides accounting services).

(8) **'recipient'** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

(9) **'personal data breach'** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

So, when personal data, accidentally or not, are unlawfully processed by a person or an entity that is not the person himself/ herself, the Data Controller or Data Processor then we have a breach.

(10) **'supervisory authority'** means an independent public authority which is established by a Member State

(11) **'cross-border processing'** means either:

(a) processing of personal data which takes place in the context of the activities of establishments in more than one Member State of a controller or processor in the Union where the controller or processor is established in more than one Member State; or

(b) processing of personal data which takes place in the context of the activities of a single establishment of a controller or processor in the Union but which substantially affects or is likely to substantially affect data subjects in more than one Member State.

(12) **'Data Protection Officer' or 'DPO'**: the person who is designated by a data controller and holds the position and duties defined by the GDPR

Co-funded by the European Union

2.4 Status and role of enforcement agents

The wording 'Enforcement Law' is used in this manual as a generic term covering the legislation regarding the organization of enforcement and enforcement proceedings in the respective Member States.

The definition of an «enforcement agent» is a generic term which covers a wide variety of persons (e.g., enforcement officer, enforcer, huissier de justice, enforcement judge etc.) who have in common an authorization by the state to carry out the enforcement process.

According to the comparative report «Civil enforcement in the EU: a comparative Overview»[2], their role, responsibilities, organization and professional status vary considerably as do their working conditions and remuneration: in the majority of EU member States, enforcement agents are either:

(1) enforcement agents subordinated to the courts,

(2) civil servants subordinated to the Ministry of justice, or

(3) self-employed persons acting independently.

The three dominant models are the following:

1. Court enforcement

The model where enforcement professionals are court enforcement agents, directed by a judge and enforcement activity is accomplished generally by courts with or without interference of the executive branch.

2. Civil servant-based enforcement

The model where enforcement professionals are civil servants and the organisation of enforcement activity is dealt with outside the courts, for example through the Ministry of Justice.

3. Self-employed enforcement

The alternative model where enforcement professionals are independent, and enforcement activity is dealt with outside the courts on a self-employed, entrepreneurial and competitive market level.

[2] M. Mousmouti, H. Meidanis and Jos Uitdehaag, *Civil enforcement in the EU: a comparative Overview,* 2021, ch. II, para 2.1, https://www.enforcementatlas.eu/wp-content/uploads/2021/03/EU-Enforcement-Atlas-Comparative-Report.pdf

Co-funded by the European Union

There are significant differences between the enforcement agent as a civil servant and the (growing trends in Europe of) the self-employed enforcement agent.

Depending on their specific status, their role while processing personal data is also different. In specific, when they are part of the personnel of courts or other services, those authorities are the data controllers and should provide instructions and guidelines on the processing, the specific policies and measures, so the officers cannot decide on their own how they will process personal data and which specific measures they will take. On the other hand, **when they are self-employed, they are data controllers on their own and should take the measures and abide by the rules of the GDPR, taking the relevant responsibility.**

For the purposes of this guide, the terms «enforcement officers», «enforcement agents», «judicial officers» and «bailiffs» will be used equally, clarifying that the guide **concerns mainly the self- employed ones who decide how exactly they process personal data and are considered as Data Controllers**.

In any case all enforcement agents should take into account that first of all they must always follow the specific rules procedures and legal framework of their country.

3. Data protection and civil enforcement: the basics

3.1 The role of the enforcement agent in GDPR

In enforcement proceedings, the enforcement agent processes personal data, as received from the client (e.g., creditor). Regarding the processing of such personal data, It is important to determine the relationship between the creditor and the enforcement agent who has the responsibility for the processing of the personal data. Depending on the role of each party (controller, processor, joint controllers) there are different obligations under the GDPR. So, it is important to determine who in this relationship is considered the controller and who is considered the processor (or if they are joint controllers) (article 4 par. 7 and 26 GDPR).

Article 4 par 7 GDPR defines the **controller** as the 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. The processor is defined (see article 4 par 8 GDPR) as a a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller. The processor does not make any decisions

Co-funded by the European Union

regarding the data, methods to use to data, access to the data or transfer of data to third parties.

The enforcement agent can be considered the controller [under specific conditions, as described above].

The processing in enforcement proceedings namely can be considered necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

The Law on Enforcement assigns the enforcement agent an explicit legal authority to execute enforceable documents. It is also the enforcement agent who decides on the method(s) of processing the data, within the relevant legal framework, as received from the client. Furthermore, it is also the enforcement agent who collects any additional data, if necessary.

GDPR leaves it up to the legislation of the member state to govern the lawfulness of the processing of data: (article 6 par 3 under b GDPR): such legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations.

In the case of joint controllers, both parties are jointly and severally liable for compliance with the Regulation. This might be the case, for example, if the enforcement agent receives an enforcement case from another enforcement agent, or in case the enforcement agent receives a case from a lawyer. In such case of joint controllers, both are jointly and severally liable for compliance with the GDPR.

The enforcement agent has the authority and the obligation to check the accuracy of personal data in the preparation of an official act. From that moment on, the enforcement agent is responsible for the accuracy of the data.

The data subject can hold the enforcement agent accountable for the lawful processing of his personal data (e.g., storage of data subject's personal data) and can also address the enforcement agent to exercise his rights.

3.2 What is personal data and how is it relevant to civil enforcement?

Personal data means any information relating to an identified or identifiable natural person ('data subject') and can be distinguished into:

Co-funded by the European Union

(a) Simple personal Data: personal data concerning the name, name of father, date of birth, address of the person, age, tax registration number, tax registration office, land registry and/ or cadaster entries, bank accounts.

(b) Special categories of personal data: personal data revealing racial or ethnic origin (e.g., nationality), political opinions, religious (e.g., religion) or philosophical beliefs, or trade union membership, and the processing of genetic data (e.g., employee's medical certificate in order to receive an absence from work), biometric data for the purpose of uniquely identifying a natural person (e.g., use of finger print in order to enter premises). Under the previous legislation special categories of personal data were known as sensitive categories of data. This term is no longer used by GDPR. Each member of the Union can specify the rules for the processing of special categories of personal data. For example, in Netherlands, sensitive data are considered: social security number, financial data, data about debts, criminal data, work or relationship problems, usernames, identity documents. In Greece social security number (AMKA) is considered as sensitive data only in cases where it is connected to a patient history.

'**Genetic data'** means personal 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' means personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

'**Data concerning health'** means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;

During the day-to-day tasks of an enforcement agent, processing of special categories of personal data is not very common. A usual case may be processing personal data by viewing them only on documents/ lawsuits that are being served. An enforcement agent does not collect, store or process personal data written on a clients legal document in any other way and there is no legal basis to justify otherwise (e.g., legal document petition for guardianship).

Co-funded by the European Union

3.3 Processing personal data in enforcement work

As already established, according to GDPR "processing' means any course of action which includes personal data. From an enforcement agents' perspective, this could mean any and all of the following examples:

- writing a service report which includes personal data on both the officer's client and the client's opponent
- writing an inventory record of debtor's possessions
- issuing copies from a service report
- keeping record of service reports for a specific period of time (either electronically or hard copy or both)
- writing a report after conducting an inspection of mortgage securities on the properties of a specific person on the competent cadestry/ land registry office
- publishing an abstract of a legal document (lawsuit, decision) when the opponent's address is not known.

In order to perform their duties, enforcement agents can process information provided by their clients (e.g., address/ phone number of the debtor), and/ or acquire necessary information from public data bases [e.g., Business Public Records/ Records of the competent Chamber of Commerce, cadastral services (for enforcement agents)]. In both cases enforcement agents process personal data in compliance with each country's applicable legal framework. The role of the enforcement agent as a controller obliges him/her to be transparent regarding the received data and its use towards the data subjects (parties). This requires the development of privacy statements towards data subjects (e.g., creditors and debtors), which include:

Informing the Creditor on the processing of the received data in the enforcement case as a controller.

Informing the Creditor on the sole responsibility of the enforcement agent regarding the methods and use of the received data, correction of received data and collection of additional data and accuracy of the data. Such responsibility is based on the legal framework for enforcement (including the independent position of the enforcement agent in enforcement proceedings).

Informing parties on the existence of a register of data breaches and procedures on data breaches.

[e.g., Informing about an office's measures regarding privacy (designated data protection officer, processing operations, the categories of data which are processed, the legal bases, the purposes and the ways for exercising the rights of the debtor as a data subject].

Co-funded by the European Union

3.4 What type of activities are considered as data processing?

Data processing covers a wide range of operations performed on personal data, including by manual or automated means.

'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data.

According to the European Commission[3], examples of processing include:
i. staff management and payroll administration;
ii. access to/consultation of a contacts database containing personal data;
iii. sending promotional emails*;
iv. shredding documents containing personal data;
v. posting/putting a photo of a person on a website;
vi. storing IP addresses or MAC addresses;
vii. video recording (CCTV).

In the case of judicial officers, data processing may include for example:

searching and collecting the receiver's or the debtor's data
entry of these data in files or applications
writing and storage of relevant reports
transmission to authorities such as the police or the court
sending copies of their reports to their clients or lawyers.

3.5 What is the legal basis for data processing in the context of enforcement of civil claims?

When the enforcement agent processes personal data of their clients, the legal basis for data processing in the context of enforcement may be either compliance with a legal obligation (Article 6.c of the GDPR) depending on the specific legal framework of each country, or the performance of a task carried out in the public interest or in the exercise

[3]https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_en

Co-funded by the European Union

of official authority vested in the controller (Article 6.e of the GDPR), depending on the specific legal framework of each state and the specific employment or service relationship.

Furthermore, an enforcement agent who has employees, signs contracts of employment with them (e.g., secretary, trainee officers, etc) and collects their documents. This record also includes some personal data: Name, date of birth, marital status (for providing benefits), male/female, tax registration number, address, bank account [depending on the specific legal framework]. All these data are necessary for the employer in order to sign this contract and fulfil the legal obligations. So, the officer or the officer's company is also considered as the Data Controller concerning the employees' data. It is suggested that employees should also sign an annex of their contract, concerning: processing of their personal data by the employer, proper information about the measures ensuring a secure and safe process of other people's personal data during the employees' tasks (technical and organizational measures), their rights based on the GDPR Regulation and the local legislation and other clauses about confidentiality. In addition, every employee should have a separate account and set strong passwords, which they will not share with any of the other colleagues.

3.6 Purpose limitation: are you allowed to use data from other cases concerning the same debtor?

All personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ('purpose limitation').

In addition, specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.

Furthermore, in case of processing personal data **for other purposes**, **such as in case of using data from other cases concerning the same debtor**, where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society, the controller should, in order to decide **whether processing for another purpose is compatible with the purpose for which the personal data are initially collected**, take into account:

a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
c) the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed;

Co-funded by the European Union

d) the possible consequences of the further processing for data subjects;
e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

The design of the processing should therefore be shaped by what is necessary to achieve the purposes. If any further processing takes place, the **controller must first make sure that this processing has purposes compatible with the original ones and design such processing accordingly**.

Key design and default purpose limitation elements may include:

- **Predetermination** – The legitimate purposes shall be determined before the design of the processing. *The enforcement agent should know in advance for which reason they will process personal data.*
- **Specificity** – The purposes shall be specified and explicit as to why personal data is being processed. *The enforcement agent should know in advance which personal data are necessary in order to fulfil their obligations.*
- **Purpose orientation** – The purpose of processing should guide the design of the processing and set processing boundaries.
- **Necessity** – The purpose determines what personal data is necessary for the processing. For example, the officer should not collect and keep copies of the entire lawsuits after being served.
- **Compatibility** – Any new purpose must be compatible with the original purpose for which the data was collected and guide relevant changes in design.
- **Limit further processing** – The controller should not connect datasets or perform any further processing for new incompatible purposes. For example, the officer should not give information of a debtor to someone who wants to cooperate with them and calls in order to know about their credit rating.
- **Limitations of reuse** – The controller should use technical measures, including hashing and encryption, to limit the possibility of repurposing personal data. The controller should also have organisational measures, such as policies and contractual obligations, which limit reuse of personal data.
- **Review** – The controller should regularly review whether the processing is necessary for the purposes for which the data was collected and test the design against purpose limitation.

Co-funded by the European Union

Example:
In Greece, in case of conducting an electronical survey upon the properties of a person via cadastral services there is a distinction according to the profession of each user (enforcement agents, engineers, lawyers, notaries). Each one of them can "see" during the online search all or certain of the available information concerning a property. For example, an enforcement agent can perform an online search in the cadastral records within the Appeal Court for which he performs his duties[4] and has access to the mortgages, a lawyer can perform an online search in the cadastral records within the country and has access to the mortgages and a notary can only perform an online search in the cadastral records within the country without having access to the mortgages of a property. This distinction has been made by design and by default in order to secure data minimization and more specifically in order to secure that each professional will have access only to the sufficient information for fulling their duties. This purpose limitation should also apply to the respective search in the cadastry's or land registry's physical records.

3.7 Retention period [Storage limitation]

Although GDPR does not state specific retention periods, article 5 par 1e GDPR states that data kept in a form **which permits identification of data subjects** cannot be kept for a longer period than is necessary for the purposes for which the personal data are processed [storage limitation]. A case where personal data may be stored for longer periods is for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. The enforcement agent should make a relevant provision in the office's privacy policy with key points such as:

- determination in advance by the controller how long the personal data will be stored. If this is not possible, at least the criteria for determining the retention period shall be determined.
- indication of the retention periods in accordance with the record of processing activities.

The following remarks can be made:

- With regard to the retention period, attention will need to be given to the different periods of the statute of limitation (these periods might differ e.g., for a consumer case, labor case, fines, etc.). Moreover, interruption of the statute of limitation

[4] https://www.gov.gr/en/ipiresies/periousia-kai-phorologia/ktematographese/uperesies-ktematologiou-gia-dikastikous-epimeletes

might lead to a new limitation period that starts. As long as a claim is not time-barred, personal data might be of importance (e.g., evidence).
- Enforcement agents can be held liable by the client, the debtor or third parties for alleged professional errors, in which case they must be able to defend himself against them.
- Enforcement agents are subject to monitoring and control. For the purposes of such control, data will also need to be stored a certain time.
- The principle of (cost) proportionality might imply that the enforcement agent uses information from archived files or pending files on the same debtor.

Retention period of official acts: the retention period for official acts is regulated by national legislation.

It is important to realize that, in addition to the use of personal data, for enforcement purposes, the office of the enforcement agent also keeps/ processes other data to which GDPR applies. Retention periods for such data might also differ depending on national law. For example:

- Tax data: tax administration will demand from the enforcement agent to keep financial data for tax purposes for a certain time period.
- Personnel data: (for example payroll tax statements for the staff, employees 'files (which might include not just the HR data, but also travel expenses,)].
- Camera surveillance
- Visitor registration

3.8 Data minimization: how much data can you use to pursue a claim?

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization').

For example, an enforcement agent should write on his report only the name, address, tax registration number of the client whose legal document is being served and the name, address, tax registration number of the receiver [according to each specific law], but not his profession or employment status (e.g., unemployed).

As a result, the enforcement agent as Data Controller [when self-employed and not as an employee] has to predetermine which features and parameters of processing systems and their supporting functions are permissible. Data minimisation substantiates and operationalises the principle of necessity. In the further processing, the controller should periodically consider whether processed personal data is still adequate, relevant and necessary, or if the data shall be deleted or anonymized.

Co-funded by the European Union

Controllers should first of all determine whether they even need to process personal data for their relevant purposes. The controller should verify whether the relevant purposes can be achieved by processing fewer personal data, or having less detailed or aggregated personal data or without having to process personal data at all[5]. Such verification should take place before any processing takes place, but could also be carried out at any point during the processing lifecycle.

Minimising can also refer to the degree of identification. If the purpose of the processing does not require the final set of data to refer to an identified or identifiable individual (such as in statistics), but the initial processing does (e.g., before data aggregation), then the controller shall delete or anonymize personal data as soon as identification is no longer needed. Or, if continued identification is needed for other processing activities, personal data should be pseudonymized to mitigate risks for the data subjects' rights.

Key design and default data minimisation elements may include:

- **Data avoidance** – Avoid processing personal data altogether when this is possible for the relevant purpose.
- **Limitation** – Limit the amount of personal data collected to what is necessary for the purpose. For example, do not receive and keep copies of other documents related to a lawsuit.
- **Access limitation** – Shape the data processing in a way that a minimal number of people need access to personal data to perform their duties, and limit access accordingly. For example, an officer's assistant should have access only to the necessary documents such as the drafts of the reports of the officer, depending on the specific tasks that they have expressly undertaken.
- **Relevance** – Personal data should be relevant to the processing in question, and the controller should be able to demonstrate this relevance.
- **Necessity** – Each personal data category shall be necessary for the specified purposes and should only be processed if it is not possible to fulfil the purpose by other means.
- **Aggregation** – Use aggregated data when possible.
- **Pseudonymizatio**n – Pseudonymize personal data as soon as it is no longer necessary to have directly identifiable personal data, and store identification keys separately. For example, give to every client a specific number/ code and keep copies of the documents related to them in files named with this number/ code.
- **Anonymization and deletion** – Where personal data is not, or no longer necessary for the purpose, personal data shall be anonymized or deleted.

[5] Art. 5(1)(c) GDPR. 37 Recital 39 GDPR so states: "...Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means."

Co-funded by the European Union

- **Data flow** – The data flow should be made efficient enough to not create more copies than necessary.
- **State of the art** – The controller should apply up to date and appropriate technologies for data avoidance and minimisation.

Additional examples:
1. In case of gathering statistical information, in order for example to make proper choices on changes concerning the procedures of enforcement, since it is not necessary for the purpose of optimizing the procedures, the controller should not store the data that identify people. In cases where there can still be a risk of identifying a person, the controller implements statistical measures to reduce the risk, such as removing those personal data.
2. The group of people with access to a debtor's file should be either enlarged or reduced to a small group of judicial officers or other officers based on the purpose and everybody's duties.

3.9 What are special categories of data? Are there any additional safeguards you need to keep in mind if processing this type of data?

Special categories of personal data include personal 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. They should be processed under specific legal bases different than those for the rest of the (simple) data.

In the case of the enforcement agents, the appropriate legal bases in order to process clients' personal data of special categories may be either legal basis (f) or legal basis (g) of article 9 of the GDPR which means in case: (f) processing is necessary for the establishment exercise or defense of legal claims or whenever courts are acting in their judicial capacity; or (g) processing is necessary for reasons of 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.

Co-funded by the European Union

In case that these two bases are not applicable, the officer may request an explicit consent in order to process sensitive data, only if this is absolutely necessary and cannot be avoided.

There are several ways to ensure consent from which one can choose depending on the occasion and the processing. **For example when someone wants to subscribe to newsletters**, the consent can be given by a checkbox and confirmation via email. But consent can also be given in natural form, by signing a document.

But what about special categories of the personnel's personal data? The enforcement agent, as an employer and Data Controller may also process special categories of the personnel's personal data (eg health data) when medical declarations are provided in order to justify the absence from the work (e.g. his secretary is diagnosed with Covid- 19, in order to take a leave of absence should provide to the employer a positive test result which contains information about his health along with his name, age, social security number, date of birth, etc). The employer should keep this in the secretary's employment record for some period. There is also the possibility that the enforcement agent (Data Controller) is obliged to send this information (positive test result) to the local social security office/ organisation in order for the employee to receive illness allowance.

In any case, the general principles of "purpose limitation" and "data minimization" should be taken into account in case of processing personal data of special categories. More specifically, if it is not necessary to collect or keep those personal data and the enforcement agent's purpose can be achieved only by keeping the basic personal data, for instance name, surname, address, etc, they should not select and use the rest.

3.10 What are the rights of the subjects whose data you are processing? What do you need to do to help them exercise them?

Any natural person- data subject (client, employee, colleague, etc.) has the following rights:

i. **Right of access (article 15 GDPR):** obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data, by providing a copy of the personal data undergoing processing.
ii. **Right to rectification (article 16 GDPR):** obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.
iii. **Right to erasure ('right to be forgotten') (article 17 GDPR)** : obtain from the controller, who is obliged to do so, the erasure of personal data concerning him or

Co-funded by the European Union

her without undue delay where one of the following grounds applies: (a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b)the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing; (c)the data subject objects to the processing and there are no overriding legitimate grounds for the processing (d)the personal data have been unlawfully processed; (e)the personal data have to be erased for compliance with a legal obligation; (f)the personal data have been collected in relation to the offer of information society services.

However, the Controller is not obliged to satisfy the data subject's request for erasure of personal data to the extent that processing is necessary:

(a)for exercising the right of freedom of expression and information;

(b)for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; For example, if the officer is obliged by a specific country's law to keep records for ten years, they cannot delete them before this period.

(c)for reasons of public interest in the area of public health

(d)for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes or

(e) for the establishment, exercise or defense of legal claims.

iv. **Right to restriction of processing (article 18 GDPR**): obtain from the controller restriction of processing (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, he 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 defense 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). Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

v. **Right to data portability (article 20 GDPR)**: The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a

Co-funded by the European Union

controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

vi. **Right to object (article 21 GDPR)**: on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims.

vii. **Automated individual decision-making, including profiling (article 22 GDPR)**: he data subject shall have the right 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.

Modalities should be provided for facilitating the exercise of the data subject's rights under the Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The Controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means.

The Controller should be **obliged to respond to requests from the data subject without undue delay and at the latest within one month** and to give reasons where the controller does not intend to comply with any such requests.

3.11 Do you need a DPO?

When the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity[6], where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data (article 9) and data relating to criminal convictions and offences (article 10), a person with expert knowledge of data

[6] Note that under Article 37(4), Union or Member State law may require the designation of DPOs in other situations as well., Guidelines on Data Protection Officers ('DPOs') Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017 [https://ec.europa.eu/newsroom/article29/items/612048]

Co-funded by the European Union

protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation.

When an enforcement agent belongs to Court enforcement or is a Civil servant or part of the personnel of courts or other services, they do not need to designate a Data Protection Officer (DPO).
When an enforcement agent is self-employed, they undertake the role of Controller and should consider the possibility to appoint a Data Protection Officer (DPO).
In most cases when someone is self-employed a DPO is not necessary to be appointed. It's a different case when there is a company of many enforcement agents.
Even if the designation of a DPO is not mandatory, entities may sometimes find it useful to designate a DPO on a voluntary basis[7].

3.12 Why GDPR?

GDPR provides a homogeneous legal framework for all the state members of the European Union, has also immediate effect to all of them and does not to be incorporated to the legal framework of each state in order to be enforceable. By GDPR, EE achieved to enforce a common and more coherent data protection framework to all her geographic territory, i.e., to all the state members, which corresponds better to all the technological developments and to the freedom of persons to travel and work within the borders of the EE.

3.13 Are there other laws or regulations you should keep in mind?

Based on the provisions of GDPR, the legal framework of the protection of personal data has been revised and has acquired solid foundations. When Controllers, Processors, Competent Authorities apply GDPR, there are many legal documents, explanatory notes, state laws, opinions, decisions that are very helpful. More specifically:

- Opinions, Decisions, Guidelines of Working Party 29, as revised
- Opinions, Decisions, Guidelines of European Data Protection Board (EDPB)
- Opinions, Decisions, Guidelines of Competent Authorities of the state members
- State members; Laws concerning personal data and GDPR (e.g., in Greece Law no 4624/2019)
- Courts' Decisions (European and state members' courts)
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in

[7] https://ec.europa.eu/newsroom/article29/items/612048 Guidelines on Data Protection Officers ('DPOs') Adopted on 13 December 2016, As last Revised and Adopted on 5 April 2017, p. 20

Co-funded by the European Union

the electronic communications sector (Directive on privacy and electronic communications)[8]

- Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws[9].
- Treaty on European Union (Article 6)[10]
- European Convention on Human Rights (Article 8)[11]
- Charter of Fundamental Rights of the European Union (Article 8)[12]
- Convention 108 – Council of Europe- Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28/01/1981[13].
- Modernized Convention 108 – Council of Europe- Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, Elsinore, Denmark, 17-18 May 2018[14].

Furthermore, based on GDPR, every state has its own legal framework which includes more specific provisions on certain articles and provisions of GDPR and should also be considered while processing personal data.

3.14 Key takeaway points on the application of the GDPR by enforcement agents

Enforcement agents should abide by the following 5 basic steps- points to protect personal data:

1. perform their duties based on the legislation and the specific procedures applicable in each member state
2. take into account the principle of minimization and collect/ process only the necessary data
3. take technical and organizational security measures
4. restrict access of third parties to their files (e.g. personnel or other external partners)

[8] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
[9] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136
[10] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT
[11] https://www.echr.coe.int/european-convention-on-human-rights
[12] https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:12012P/TXT
[13] https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108
[14] https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf

Co-funded by the European Union

5. sign confidentiality terms with their partners and personnel

Here is an overview of the various steps to be undertaken to implement the GDPR within the enforcement agent's office, as proposed by an enforcement officer, member of the Union Internationale des Huissiers de Justice et officiers Judiciaires:

1. Appointment of a Data Protection Officer (DPO)

In accordance with article 37 GDPR, each enforcement agent's office will either have to appoint a DPO or hire the expertise.

Document relevant: job description of the DPO (articles 37 and 38 GDPR)

2. Inventory which data are processed

Based on the GDPR, personal data need to be protected. As a first step it is important to identify what data there are, how those data are processed and wehre the data are located. This needs to be recorded in a processing register.

This means:

- making of an inventory of the applications that are used in the office (Case management system; CRM; online files; HR administration etc.)
- making of an inventory with parties with whom data are exchanged (e.g. creditors, Chamber of enforcement agents; software supplier; accountant, etc.)

Relevant document: processing register (see article 30 GDPR)

3. Determination of priorities in the office

GDPR demands that risks with regard to data protection are identified and that the enforcement agent will undertake additional steps to safeguard such protection, for example access security or encryption of data.

4. Creation of the documentation as mentioned in GDPR

Data subjects need to be informed on the data processing and compliance with GDPR. This means that a set of documentation, as mentioned in the GDPR, is available:

- Model processing agreement
- Model registry data breaches
- Model privacy statement for litigants
- Model privacy statement for clients
- Model privacy statement for employees
- Model Privacy Impact Assessment

5. Implementation of the GDPR procedures

Co-funded by the European Union

GDPR demands that each office sets up certain procedures to protect the rights of the data subject. Such procedures include reporting obligations and procedures for the handling of data breaches:

- Procedure informing / right of access to the data subject
- Right of objection procedure
- Procedure for erasing personal data
- Procedure correction of personal data
- Procedure for transferring data
- Procedure for detecting, registering and reporting data breaches
- Procedure archiving and deletion

4 DATA SECURITY

4.1 What is data security? How can it be ensured?

In order to secure the confidentiality, integrity, availability of the personal data under processing Controllers and Processors should take all the necessary and appropriate technical and organisational measures to ensure that a data breach (i.e., accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed) will not take place.

A data breach is a security incident involving personal data. Such data breach falls into one or more of these categories:

- *Breach of availability:* the data is temporarily unable to access or lost.
- *Breach of confidentiality:* access to the data has been obtained by unauthorized persons.
- *Breach of integrity:* unauthorized changes have been made to the data.

Some categories of data breaches are:

1. Unauthorized or accidental access to data - breach of confidentiality (e.g. identity theft following the disclosure of the pay slips of all employees of a company);

2. Unauthorized or accidental alteration of data - breach of integrity (e.g. falsely accusing a person of a wrongdoing or crime as a result of the modification of access logs);

3. Loss of data or loss of access to data - breach of availability (e.g. failure to detect a drug interaction due to the impossibility of accessing the patient's electronic record).

Co-funded by the European Union

4.2 What is data protection by design and by default?

Each officer as data controller, in order to be able to demonstrate compliance with the GDPR, should implement all the appropriate technical and organisational measures, both at the time of the determination of the means for processing and at the time of the processing itself.

More specifically, such measures could consist, inter alia, of minimizing the processing of personal data, pseudonymizing personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders. For example, when controller chooses a cloud provider for storage or an application for invoicing should examine all the technical and organizational measures taken by the provider for his compliance with GDPR.

Article 25 GDPR also applies in Small & Medium Size Entities, such as , which are strongly advised to abide by the following points in order to facilitate their compliance with GDPR provisions:

➢ Do early risk assessments
➢ Start with small processing – then scale its scope and sophistication later
➢ Look for producer and processor guarantee, such as certification and adherence to code of conducts
➢ Use partners with a good track record
➢ Talk with DPAs (Data Protection Authorities)
➢ Read guidance from DPAs and the EDPB
➢ Adhere to codes of conduct where available
➢ Get professional help and advice[15]

[15]Guidelines 4/2019 on Article 25 Data Protection by Design and by Default available on https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en link

Co-funded by the European Union

4.3 What type of measures do you need to apply to ensure the security of physical files?

These are some recommended measures concerning physical files:

- only the authorized personnel should have access to the places where personal data are stored and/ or processing
- installation of CCTV
- installation of Fire extinguishing system
- use of furniture where locks can be placed
- digital copies of the physical files
- use of a record destructor for destruct documents on a small scale & use of a certified company for destruct documents and physical files on a large scale
- The service by affixing notice should be given in a sealed envelope with the enforcement agent's stamp and the name of the specific person to whom it is addressed.
- Staying informed and training also the personnel about privacy related risks (accidental disclose of personal data by not using a clean desk policy)

4.4 What type of measures do you need to apply to ensure the security of digital files?

The GDPR does not contain specific security measures that controllers and processors must implement, but they should take into account:

- the latest developments in technology,
- the cost of implementing security measures,
- the characteristics of the processing (nature, scope, context and purposes of processing),
- the risks to the rights and freedoms of natural persons from the processing, taking into account for each risk the different probability of its realization and the seriousness of the consequences, if it occurs.

Article 32 of the GDPR proposes "appropriate" technical and organizational security measures: Pseudonymization and Encryption, ensuring Privacy, Integrity, Availability and Reliability, Restoration of Availability and access in the event of an incident, Process for testing, assessing and continuously evaluating the effectiveness of measures.

In specific, these are some recommended measures concerning digital files:

➢ strong passwords that change periodically (password manager can be used if needed)
➢ multi-factor authentication

Co-funded by the European Union

➢ encryption of sensitive files and hard drives. This means that the officers should keep encrypted USB sticks including their client's files or encrypted files in their laptops, because in case of loss or stealing those files cannot be read by a third party.
➢ attention when transmitting files over the internet
➢ back up of important files regularly in multiple locations
➢ installation of reputable anti-virus and anti-malware software to detect and remove threats
➢ attention on attachments or files from untrusted sources
➢ firewalls, ad blockers and other security layers that help prevent unauthorized access keeping all software up-to-date
➢ access restrictions where possible
➢ Install a VPN for telework
➢ Up-to-date access permissions, firewall and antivirus, backup storage for users
➢ Training on information security
➢ Telework safety policy

4.5 Who in your office can have access to your file? How do you prevent access from unauthorized personnel?

Access to your files should be limited depending on who in necessary to have access to them, in order to fulfil your obligations and duties. For example, the personnel who is dedicated to a specific task and needs to have access to some documents or colleagues with whom you have a specific agreement to cooperate, in compliance with the GDPR.

In specific, these are some recommended measures concerning limited access:

➢ access controls and permissions
➢ access only to personnel that need it for their tasks/ duties
➢ avoid shared servers
➢ in case of using a shared server, different user accounts for each employee and different permissions on folders to restrict access
➢ limitation of rights (view, edit, etc.)

Co-funded by the European Union

➢ extra encryption, password protection or other access restrictions beyond network permissions depending on the data in each file
➢ strong passwords
➢ screen locking
➢ session timeouts that log users off applications/servers after a period of inactivity.
➢ security software that can generate logs of who accessed what and when
➢ physical security of computers, servers and storage devices
➢ locked rooms or cabinets
➢ policies against unauthorized file access and procedures for reporting incidents
➢ when employees leave your company/ when a cooperation with another colleague terminates, their network, server and application access rights should also be terminated
EXAMPLES
If the officer's secretary works only on writing the drafts of their reports, it is not necessary that they have access to the whole survey and results concerning the debtor's property. If many officers share one office but have different clients, each of them should have access to their clients' files and data.

4.6 What type of measures do you need to apply to ensure network and communications security?

These are some recommended measures concerning network and communications, in combination with the above measures:

➢ encryption and VPNs, to protect data in transit over networks and the internet. firewalls to filter traffic and block malicious connections
➢ intrusion detection and prevention systems, to identify and stop exploits, malware and cyberattacks targeting the network
➢ updated software on networked devices
➢ strong passwords and multi-factor authentication for network and system access

Co-funded by the European Union

➢ control access to networks and critical infrastructure via user accounts, permissions and physical controls
➢ logs and monitoring of network activity
➢ isolation of sensitive networks and implementation of demilitarized zones
➢ cybersecurity training to employees/ partners
➢ incident response plans to quickly detect network breaches or malicious attacks
➢ network tests and audits for vulnerabilities via pen testing, scans and risk assessments.

4.7 What is the Record of Processing Activities (Art. 30 GDPR)? When do you need to have one and what is its minimum content?

Most entities are required to keep a record describing their personal data processing activities. This file is not important only as an obligation according to Article 30 GDPR but also because it is useful for the proper entity, in order to organize the procedures of the personal data processed.

The data controllers and processors are obliged to keep this file, each with different details.

An entity employing more than 250 people must keep a record of every activity. However, an entity employing fewer than 250 people, such as an enforcement agent's office or company, must keep a record of any activity that:

- is likely to result in a risk to the rights and freedoms of data subjects,
- is not occasional, or
- includes special categories of data or personal data relating to criminal convictions and offences.

This means that even enforcement agents' companies should keep such a record, based on the details of GDPR and the examples of each state's data protection authority.

According to the members of the Union Internationale des Huissiers de Justice et officiers Judiciaires, the primary processing in the enforcement agent's office are all actions in the files of the enforcement case management system. However, also other data are processed in the office. For example: the personnel administration, camera surveillance, trip registration and the registration list of visitors. In all these cases personal data are processed.

Co-funded by the European Union

The Record of processing activities aims to raise the awareness of the organizations on the use of the personal data they collect and use, the systems that are used and the security measures around it. GDPR prescribes which information must be included by the controller in the register as a minimum:

- Name and contact details of the controller (e.g., the enforcement agent or company)
- Name and contact details of other organizations with whom the purposes and means of the processing may have been jointly determined
- Name and contact details of the Data Protection Officer (DPO)
- Purposes for which the personal data are processed
- Description of the categories of the data subjects (such as debtor, employee, administrator)
- Description of the categories of personal data (such as BSN, name and address details, telephone numbers, camera images or IP addresses)
- Categories of recipients to whom you provide personal data
- Retention period
- Indicate the name and contact details of any international organizations with which you share personal data if they are located outside the European Economic Area
- General description of the technical and organizational measures relating to the security of personal data

As additional information one may mention:

- Systems into which certain data is processed
- Sources of the data

Bases for the processing of data:

Article 6 GDPR mentions six bases for the processing of personal data:

(a) the data subject has consented to the processing of his or her personal data for one or more specific purposes

(b) processing is necessary for the performance of a contract to which the data subject is a party or for taking measures at the request of the data subject prior to the conclusion of a contract

c) the processing is necessary to comply with a legal obligation to which the controller is subject

(d) the processing is necessary to protect the vital interests of the data subject or of another natural person

Co-funded by the European Union

(e) 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

(f) processing is necessary for the purposes of defending the legitimate interests of the controller or of a third party, except where the interests or fundamental rights and freedoms of the data subject which require the protection of personal data outweigh those interests, in particular where the data subject is a child

Each processing operation includes the data types used in that processing. This only concerns personal data.

For each data type, the following information is available:

- Data subject: Who the personal data concerns, of whom is it personal data
- Basis: On what legal basis is this type of data processed.
- Source: Where does the data come from
- Processors: Which party or parties (suppliers) process the data on your behalf.
    - Obvious example is the supplier of the CMS.
- Recipients: To whom are the data provided
- Systems: Which software applications are used in the data processing
- Retention period: What is the general retention period of the data type
- Security: What measures have been taken to secure the data

Here are some examples how this is considered in practice (based on the Dutch Handbook on the application of the GDPR) for the processing of data in case of an attachment of movable goods:

1. the attachment of the movable goods

Owner:	enforcement agent
Basis of the data processing:	carrying out a task in the public interest

Data:	file number
Basis for the data processing:	carrying out a task in the public interest
Data subject:	debtor
Source:	File
Recipient:	
Processor:	software application deliverer
System:	Software application

Co-funded by the European Union

Security:	Access rights, user identification, firewall, pass word management, secure connection, access security, malware protection
Retention period:	10 years after closing of the file

Data:	Act of seizure of the movables
Basis for the data processing:	carrying out a task in the public interest
Data subject:	debtor
Source:	File
Recipient:	
Processor:	software application deliverer
System:	Software application
Security:	Access rights, user identification, firewall, pass word management, secure connection, access security, malware protection
Retention period:	10 years after closing of the file

Data:	Data of birth
Basis for the data processing:	carrying out a task in the public interest
Data subject:	debtor
Source:	File
Recipient:	
Processor:	software application deliverer
System:	Software application
Security:	Access rights, user identification, firewall, pass word management, secure connection, access security, malware protection
Retention period:	10 years after closing of the file

Data:	Name
Basis for the data processing:	carrying out a task in the public interest

Co-funded by the European Union

Data subject:	debtor
Source:	File
Recipient:	
Processor:	software application deliverer
System:	Software application
Security:	Access rights, user identification, firewall, pass word management, secure connection, access security, malware protection
Retention period:	10 years after closing of the file

Data:	Address and domicile
Basis for the data processing:	carrying out a task in the public interest
Data subject:	debtor
Source:	File
Recipient:	
Processor:	software application deliverer
System:	Software application
Security:	Access rights, user identification, firewall, pass word management, secure connection, access security, malware protection
Retention period:	10 years after closing of the file

Data:	Judgment
Basis for the data processing:	carrying out a task in the public interest
Data subject:	debtor
Source:	File
Recipient:	
Processor:	software application deliverer
System:	Software application
Security:	Access rights, user identification, firewall, pass word management, secure connection, access security, malware protection
Retention period:	10 years after closing of the file

Co-funded by the European Union

2. Processing of the act of seizure of the movables

Data:	code of employee
Basis for the data processing:	carrying out a task in the public interest
Data subject:	debtor
Source:	File
Recipient:	
Processor:	software application deliverer
System:	Software application
Security:	Access rights, user identification, firewall, pass word management, secure connection, access security, malware protection
Retention period:	10 years after closing of the file

File number et cetera

Name et cetera

Address and domicile et cetera

3. Service of the act of seizure to the debtor

Et cetera

4. Announcement of the public sale

Et cetera

5. Sequestration of the movables

Et cetera

6. Public sale

Et cetera

4.8 What is a data protection impact assessment? When and why do you need to perform it?

According to Article 35 GDPR, where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a **high risk** to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risk.

A data protection impact assessment shall in particular be required in the case of:

Co-funded by the European Union

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1) or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

Regarding (b), it can be mentioned that the Estonian DPA has proposed following criteria regarding large-scale processing (special personal data: 5,000 persons; sensitive personal data: 10,000 people; other: 50,000 people). The wording sensitive data is not used in GDPR. For example, in Netherlands, sensitive data are considered: social security number, financial data, data about debts, criminal data, work or relationship problems, usernames, identity documents.

It is the responsibility of the controller to determine the privacy risk. The controller may not start processing data with a high privacy risk before a DPIA has been carried out. The Data Protection Officer must be involved in the assessment of the DPIA. If the conclusion from the DPIA is that the processing still poses a high risk to data subjects even with the risk-reducing measures, there is an obligation to ask the DPA for an assessment and a change.

As an example: the Dutch Data Protection Authority has drawn up a list of processing operations for which the execution of a DPIA is in any case mandatory:

1. **Covert investigation:** Large-scale and/or systematic processing of personal data in which information is collected by means of research without prior notice to the data subject.
2. **Blacklists:** Processing in which personal data relating to criminal convictions and offences, data concerning unlawful or nuisance behavior or data on poor payment behavior by organizations or individuals are processed and shared with third parties.
3. **Fight against fraud:** Large-scale and/or systematic processing of (special) personal data in the context of fraud prevention. For example, fraud prevention by social services or by fraud departments of insurers.
4. **Credit scores:** Large-scale and/or systematic data processing that leads to or uses estimates of the creditworthiness of natural persons, for example expressed in a credit score.

Co-funded by
the European Union

5. **Financial situation:** Large-scale and/or systematic processing of financial data from which people's income or capital position or spending habits can be deduced. For example, statements of bank transfers, statements of the balances of someone's bank accounts or statements of mobile or debit card payments.

9. **Camera surveillance:** Systematic and large-scale monitoring of publicly accessible spaces using cameras, webcams or drones.

10. **Flexible camera surveillance:** Large-scale and/or systematic use of flexible camera surveillance. For example, cameras on clothing or helmet of fire or ambulance personnel, dashcams used by emergency services.

11. **Employee control:** Large-scale and/or systematic processing of personal data to monitor employee activities. For example, checking e-mail and internet use, GPS systems in employees' (freight) cars or camera surveillance for theft and fraud prevention.

12. **Location data:** Large-scale and/or systematic processing of location data of or traceable to natural persons. For example, by (scanning) cars, navigation systems, telephones, or processing location data of travelers in public transport.

13. **Communication data:** Large-scale and/or systematic processing of communication data including metadata traceable to natural persons, unless and insofar as this is necessary to protect the integrity and security of the network and service of the provider concerned, or the end user's peripheral device.

15. **Profiling:** Systematic and comprehensive assessment of personal aspects of natural persons based on automated processing (profiling). For example, assessment of professional performance, student performance, economic situation, health, personal preferences or interests, reliability or behavior.

4.9 When do out have a data breach? What do you need to do in the event of a data breach?

As part of any attempt to address a breach the controller should first be able to recognize one[16]. The GDPR defines a “personal data breach” in Article 4(12) as: “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.”
In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorized according to the following three well-known information security principles:

[16] See Guidelines 9/2022 on personal data breach notification under GDPR version 2.0, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en

Co-funded by the European Union

➢ "Confidentiality breach" - where there is an unauthorized or accidental disclosure of, or access to, personal data. ***EXAMPLE: access of unauthorized personnel or colleagues to files and lawsuits***
➢ "Integrity breach" - where there is an unauthorized or accidental alteration of personal data. ***EXAMPLE: access to electronic files and changes on the debtors' details***
➢ "Availability breach" - where there is an accidental or unauthorized loss of access18 to, or destruction of, personal data. ***EXAMPLE: Data has been deleted either accidentally or by an unauthorized person, or, in the example of securely encrypted data, the decryption key has been lost.***

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

Some examples of infringements on data protection provided by a member of Union Internationale des Huissiers de Justice et officiers Judiciaires:

- sending data (confirmation a payment in instalments, status overview in a file, a copy of a letter, management overviews for the creditor) to an incorrect e-mail address
- unauthorized access to the case management system
- unauthorized access to the office
- leaving or losing a laptop, mobile phone, tablet or documents with third parties or in public spaces (train, restaurant)
- virus infection or malware in the computer system
- hacks of the case management or computer system
- passwords that fall into the hands of third parties
- a writ that ends up with a third party due to incorrect addressing

Co-funded by the European Union

Under Article 33, the GDPR requires controllers to handle every personal data breach in the context of the controllers' obligations regarding the security of processing. In case the breach is likely to result in a risk to the rights and freedoms of the persons concerned, the controllers must notify the breach in question to the supervisory Authority. A procedure for registering & reporting data breaches describes the way in which the enforcement agent acts in the event of the signal that there is (possibly) a data breach. If there is a moderate to serious data breach, where there is a risk of loss or unlawful processing of personal data, the controller must report the data breach to the national Data Protection Authority. In a number of cases, the data breach must also be reported to the data subjects.

Such notification must be made without undue delay and, where feasible, not later than 72 hours after the controller has become aware of it. The notification must contain specific information (e.g., nature/scope of the breach, categories of persons affected, cause and consequences of the breach, measures taken to address it, etc.). Even if all the above information is not available at the time of submitting the notification, the latter should be submitted as an initial notification to be subsequently updated without undue delay (by submitting a supplementary notification). If a data breach is wrongly not reported, the DPA can decide to impose a fine.

Examples
In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorized persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realized the USB key had been lost. A cybercriminal contacts the officer after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked the officer has clear evidence that a breach has occurred and there is no doubt that it has become aware.

Whilst it is the responsibility of controllers and processors to put in place suitable measures to be able to prevent, react and address a breach, there are some practical steps that should be taken in all cases.

- Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk.

Co-funded by the European Union

- Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organization being informed.
- Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.
- At the same time, the controller should act to contain and recover the breach. Documentation of the breach should take place as it develops.

Furthermore, when a breach takes place in the context of cross-border processing and notification is required, the controller will need to notify the lead supervisory authority[17].

However, breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the supervisory authority. An example might be where personal data are already publicly available and a disclosure of such data does not constitute a likely risk to the individual.

In addition, under Article 34 GDPR, when the data breach is likely to result in a high risk to the rights and freedoms of natural persons concerned, the controller must communicate the breach to those persons too without undue delay**. If the risk is difficult to be estimated by an enforcement agent or in case of doubts, they should either communicate the breach in any case, or consult experts.** Such communication is made regardless of the above-mentioned notification to the supervisory Authority (which must be submitted even if the relevant risk is not considered high). The communication to the natural persons should be made in the most appropriate and effective manner, in the form of personalized information and not by a communication of a general nature, insofar as this is possible.

However, here are three conditions that, if met, do not require notification to individuals in the event of a breach. These are:
• The controller has applied appropriate technical and organizational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorized to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
• Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialize. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be

[17] See WP29 Guidelines for identifying a controller or processor's lead supervisory authority, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

Co-funded by the European Union

given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.
• It would involve disproportionate effort to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

EXAMPLES OF BREACHES AND RECOMMENDATIONS
1. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in. As long as the data are encrypted with a state-of-the-art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However, if it is later compromised, notification is required.
2. Personal data of a large number of debtors are mistakenly sent to the wrong mailing list with 1000+ recipients. The controller should report to both the supervisory authority and the individuals, depending on the scope and type of personal data involved and the severity of possible consequences.

4.10 Restriction, correction or deletion of data

Request for correction of personal data

Article 17 GDPR ensures that the data subject has the right, under certain conditions, to obtain rectification of personal data concerning him or her without unreasonable delay. Such correction request under the GDPR only applies to personal data and has to be done in written.

Each request is registered. If necessary, the identity of the applicant will need to be verified. A correction request is rejected in case:

- There is a repeated (identical) request within a certain period
- The scope of the request remains unclear despite any further information

Co-funded by the European Union

- The request concerns data other than personal data
- Complying with the request is contrary to a legal obligation
- The request concerns personal data that the enforcement agent has received from a (mandatory) consultation of a register in the course of his duties.

In case the correction is carried out, such correction is to be carried out in all relevant (digital) systems. Third parties are informed which personal data have been corrected and these third party(s) are requested also to correct any copy of or link to that personal data. A response to the correction request is sent to the data subject.

Personal data from backups will not be corrected in the event of a correction request. When a backup is restored, all personal data present in that backup that falls under a correction request that has already been carried out is corrected again after the restore.

Request for deletion of personal data

Based on artic le 17 GDPR, the data subject has the right, under certain conditions, to obtain the erasure of personal data concerning him or her without unreasonable delay. Such request has to be done in written and shall be registered (including the date of receipt and response deadline).

If necessary, the identity of the applicant will need to be verified.

Deletion means that the data will be deleted, or the personal data will be completely and irreversibly anonymized. It only refers to the personal data. All other data (e.g., financial data or file number) will be stored in accordance with the retention periods.

Personal data from backups will not be deleted in the event of a deletion request. When a backup is restored, all personal data present in that backup that falls under a deletion request that has already been carried out is deleted again after the restore.

Request for restriction of processing personal data

Article 18 GDPR ensures that the data subject has the right, under certain conditions, to obtain the restriction of the processing of personal data concerning him or her without unreasonable delay. A request is done in written and is to be registered.

If necessary, the identity of the applicant will need to be verified.

A restriction request is rejected in case:

- There is a repeated (identical) request within a certain period
- The scope of the request remains unclear despite any further information
- The request concerns data other than personal data
- Complying with the request is contrary to a legal obligation

Co-funded by the European Union

- Compliance with the request is contrary to statutory or retention periods
- The request concerns personal data that are necessary for the handling of a complaint or objection that has been submitted to him or in which legal proceedings have been initiated.
    - If there is a restriction request from a debtor, litigant or other person involved in the file, the restriction request will in many cases be rejected for the purpose of exercising public authority and the established retention period
    - It is good practice to always submit intended rejections of restriction requests to the DPO for advice.

If the grounds for rejection do not apply, the enforcement agent assesses whether the restriction request applies:

- The personal data are no longer necessary for the purposes for which they were processed
- The data subject has previously given (explicit) permission for the use of his data, but now withdraws that consent
- The data subject objects to the processing and there are no legitimate grounds for the processing
- The personal data have been processed unlawfully
- The personal data is incorrect
- The personal data must be deleted on the basis of a legal obligation
- The data subject has objected to the processing due to special personal circumstances (Art. 21 para. 1 GDPR) and no decision has yet been taken on this objection.

In the above cases, the enforcement agent assigns the restriction request.

The enforcement agent ensures that in the event of a restore of a backup, all processing of personal data present in that backup that falls under a restriction request that has now been carried out is restricted again after the restore. He records this in the request registration.

Co-funded by the European Union

4.11 Do you need a data security policy? What are some available certification options? Is it necessary to obtain them?

Having a data security policy is critical for any data controller that handles sensitive or confidential information. A policy can regulate ore easily the usage, management, and monitoring of data. Data security policies are typically not required by law, but can help you as a data controller in order to comply with data protection standards and regulations.

As for certification, this is not necessary but useful, especially if you have employees or partners/ associates.

Some key certifications related to data security may include, depending on your specific work or collaboration framework:

- ISO/IEC 27001:2013 Offered by ISO (International Organization for Standardization)
- CISSP (Certified Information Systems Security Professional) - This credential covers a broad range of IT security topics and is one of the most widely recognized certifications. Administered by (ISC)2.
- CISA (Certified Information Systems Auditor) - Focuses on auditing and controlling information systems. Offered by ISACA. Valuable for audit, compliance and risk management roles.
- CIPP (Certified Information Privacy Professional) - Specialized certification relating to legal requirements and privacy policies. Offered by IAPP.
- CCISO (Certified Chief Information Security Officer) - Designed for CISOs and senior security executives. Covers risk management, compliance, leadership skills. By EC-Council.
- CompTIA Security+ - A good baseline security certification covering network, compliance, operational security and threats. Vendor-neutral. While certifications are not always mandatory, they demonstrate expertise and continuing education.

4.12 Ten easy steps towards compliance

i. Clauses of confidentiality for the employees, the providers and the rest of the colleagues (e.g., NDA)

ii. Inform the clients about the processing of their personal data with a standard Information Form/ Policy which can be available on your website (which data do you collect, under what legal basis, for which purpose, how long you retain them, how you destroy/ delete them, what are your clients' rights, etc)

iii. Limited access to the records/ files, according to the duties of each person involved

iv. Use of strong, complicated passwords for the computers/ digital records (e.g., 123AB is not a strong code, it is suggested to use a combination of letters, numbers, symbols, capitals)

v. CCTV in order to protect the physical records and check the entrances / exits of the rooms with critical infrastructure, based on the legal framework and the guidelines

Co-funded by the European Union

of each data protection authority on CCTV (e.g., computer room, storage, back-ups, etc)

vi. Taking digital back-ups every day, in order to ensure that the data will be available

vii. Use encrypted files and encrypted USB sticks

viii. Take basic security measures such as antivirus

ix. Destroy personal data after the period during which you are obliged to keep records, according to each state's legal framework

x. Use pseudonymization where possible for example have a number/ code for each client

5 DATA PROTECTION IN DIGITAL ENFORCEMENT

Enforcement professionals are strongly impacted by the digitalisation of justice and enforcement of court decisions, whether it is the electronic communication of documents, access to dematerialised registers, the dematerialisation of enforcement procedures, the digital management of professional activities, or the use of artificial intelligence to set up automated enforcement. In addition, new goods are appearing with digitisation (cryptocurrency for example), which forces us to think about seizure procedures adapted to these digital goods, which by their very nature are global[18].

This is critical especially for free-lancers who are not guided by an Authority on how exactly they should adapt their tasks and duties to these changes.

Certain universal principles which states should introduce into their national legislation, to govern the use of digital technology in the enforcement of court decisions and contracts are defined in the Global Code of Digital Enforcement. In specific, digital enforcement not only refers to procedural aspects of enforcement ('e-enforcement'), but also to substantive aspects ('enforcement against digital assets').

Until specific laws concerning these procedures are in force, all enforcement agents should implement small steps towards digitalisation such as electronic communication or storage of their documents, taking into account the suggested safety measures, as for example encryption in rest and in transit, strong passwords, limitations of other people's access to their files, antivirus, etc., as aforementioned.

[18] Union Internationale des Huissiers de Justice, the International Union of Judicial Officers (UIHJ), *Global Code of Digital Enforcement* [website], https://www.uihj.com/downloads-2/global-code-of-enforcement/ (accessed 23 September 2023)

Co-funded by the European Union

6 DATA PROTECTION IN CROSS-BORDER ENFORCEMENT

6.1 Can you freely transfer data within the EU, for the purposes of enforcement?

Provisions of GDPR are made in accordance with the technological breakthroughs and respective challenges. Technology and globalisation have transformed both the economy and social life, and should further facilitate not only the free travel and movement of the European citizens but also the flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

Within the EU we can "freely" transfer personal data as long as we have obtained them legally and we are processing them under a legal basis. For the purposes of enforcement, a transfer of personal data can take place under the legal basis of article 6 par. 1 (c) and more likely (e).

ATTENTION:

According to article 48 of GDPR *"Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter."*

Example:
An enforcement agent (more likely a court enforcement agent) sends (either by himself or through the competent authority) an enforceable decision, issued by a Greek court to Turkey/ India/ Mexico/ Marocco to a colleague enforcement agent in order to enforce the decision over there[19].

An enforcement agent should keep in mind that every judicial and extrajudicial service in civil and commercial case takes place under the following legal framework: (a) Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, (b) REGULATION (EU) 2020/1784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2020 on the service in the Member States of judicial and extrajudicial documents in civil or commercial matters (service of

[19] Article 10 of Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters available in https://www.hcch.net/en/instruments/conventions/full-text/?cid=17

Co-funded by the European Union

documents)[20] or (c) on the basis of bilateral agreements between states. So officers should first of all check which is the legal framework depending on the specific countries involved, follow the specific procedures provided and do not take decisions on their own about which procedure to follow and how exactly to process those personal data.

6.2 What rules do you need to keep in mind?

The main rules an enforcement agent should keep in mind are:

➢ Collect the personal data which are transferred lawfully
➢ Transfer the personal data under a legal basis
➢ Take measures to ensure data security, i.e., confidentiality, integrity, availability
➢ Apply specific technical and organisational measures (e.g., using a code to encrypt files, sending the files via email and password via SMS).
➢ Address to the competent authorities per case.

6.3 What are data transfers to third countries?

According to article 44 of GDPR, by data transfers to third countries we mean any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation. All provisions of GDPR concerning transfers of personal data to third countries or international organisations have to be applied in order to ensure that the level of protection of natural persons guaranteed by the Regulation is not undermined.

6.4 What do you need to keep in mind in enforcement procedures involving third countries? What rules apply?

In Chapter V of GDPR [articles 44 -50], step by step, are explained the rules we need to keep in mind when a transfer will occur. More specifically:

- We can **freely disclose personal data within the territory of EE**, as long as we have obtained them legally and we process them under a legal basis.
- A transfer of personal data to a **third country or an international organization** may take place where the Commission has issued **an adequacy decision** for that third country, a territory or one or more specified sectors within that third country, or that international organization. Such a transfer shall not require any specific authorization.

[20] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020R1784

Co-funded by the European Union

- If there isn't an adequacy decision, then transfer can take place only if the controller or processor has provided **appropriate safeguards,** and on condition that enforceable data subject rights and effective legal remedies for data subjects are available [e.g., binding corporate rules in accordance with Article 47, standard contractual clauses, an approved code of conduct].
- If there isn't an adequacy decision or appropriate safeguards, then transfer can take place only on one of the following conditions:

(a) the data subject has ***explicitly consented*** to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

(b) the transfer is necessary for the ***performance of a contract*** between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

(c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

(d) the transfer is necessary for ***important reasons of public interest***;

(e) the transfer is necessary for the ***establishment, exercise or defence of legal claims***;

(f) the transfer is necessary in order to ***protect the vital interests*** of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

(g) the transfer ***is made from a register*** which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

In any case, the exact procedure is determined by the legal framework applicable in the states involved.

6.5 Which foreign authorities can you expect to communicate with during cross-border enforcement procedures?

As stated, the applicable legal framework varies from state to state and so does the foreign authorities an enforcement agent should get in contact with. These foreign authorities may be (a) the competent ministry (e.g., Ministry of Justice, of Foreign Affairs, etc), (b) Courts of Justice or other competent judicial authorities, (c) competent colleagues (e.g., France), (d) Embassies.

Co-funded by the European Union

7 USEFUL RESOURCES

List of useful links (EDPB, educational material, etc.)

Primary Sources

Legislation

- Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)(2016)OJL119/1 [available at https://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679]
- Convention of 15 November 1965 on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters, article 10, [available in https://www.hcch.net/en/instruments/conventions/full-text/?cid=17]

Opinions & Guidelines by European Data Protection Board and WP29

- Guidelines 4/2019 on Article 25 Data Protection by Design and by Default available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42019-article-25-data-protection-design-and_en
- Guidelines 9/2022 on personal data breach notification under GDPR version 2.0, available at https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-92022-personal-data-breach-notification-under_en
- WP29 Guidelines on identifying a controller or processor's lead supervisory authority
- Guidelines on Data Protection Officers ('DPOs') adopted on 13 December 2016, as last Revised and Adopted on 5 April 2017

Internet/Websites

- https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32009L0136
- https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012M%2FTXT
- https://www.echr.coe.int/european-convention-on-human-rights
- https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=celex:12012P/TXT
- *https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108*
- *https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016807c65bf*
- *https://commission.europa.eu/law/law-topic/data-protection/reform/what-constitutes-data-processing_en*
- *https://www.gov.gr/en/ipiresies/periousia-kai-phorologia/ktematographese/uperesies-ktematologiou-gia-dikastikous-epimeletes*

Co-funded by the European Union

- *https://www.uihj.com/downloads-2/global-code-of-enforcement/ (accessed 23 September 2023) Union Internationale des Huissiers de Justice, the International Union of Judicial Officers (UIHJ), Global Code of Digital Enforcement [website]*
- *https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020R1784*
- *http://ec.europa.eu/newsroom/document.cfm?doc_id=44102*

Secondary Sources

Mousmouti M., Meidanis H. and Uitdehaag Jos, Civil enforcement in the EU: a comparative Overview, 2021, chapter II, para 2.1, [https://www.enforcementatlas.eu/wp-content/uploads/2021/03/EU-Enforcement-Atlas-Comparative-Report.pdf]

Co-funded by the European Union