CENTRE FOR EUROPEAN CONSTITUTIONAL LAW
THEMISTOKLES AND DIMITRIS TSATSOS FOUNDATION

International Union of Judicial Officers
Union internationale des huissiers de justice

PACE

Creating Privacy Awareness in Civil Enforcement

101090018 — PACE — JUST-2022-JTRA

Deliverable 2.1

TNA Report

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the European Commission can be held responsible for them.

Table of contents

Abbreviations

DPA	Data Protection Authority
DPO	Data Protection Officer
EC	European Commission
EDPB	European Data Protection Board
EU	European Union
GDPR	General Data Protection Regulation
EAs	Enforcement Agent(s)
MS	Member State(s)
TNA	Training Needs Assessment
ToT	Training of Trainers

Executive summary

This document presents the results of the Training Needs Assessment carried out in the framework of the PACE project. The TNA aims to identify the level of knowledge of enforcement agents from 23 EU Member States and 3 Candidate Countries (Albania, Montenegro and North Macedonia) on the EU data protection framework, as well as gaps and practical barriers to GDPR-compliant civil enforcement. The results of the TNA will serve as a solid evidence base for the development of a targeted, timely and relevant training programme for EAs, including the training of EAs as trainers.

Introduction

The project in a nutshell. The project *Creating Privacy awareness in civil enforcement – PACE* aims to contribute to the effective and coherent application of EU law in the area of civil enforcement and data protection. Specifically, the project aims to a) establish a solid evidence base on data protection challenges in civil enforcement proceedings and the training needs of Enforcement Agents (EAs) in this area; b) organise 3 3-day Train the Trainers workshops for 52 EAs from 26 EU Member States (MS) who will be trained to become trainers on data protection in civil enforcement; c) organise 10 2-day webinars for 300 EAs from 26 EU MS on EU data protection in civil enforcement; d) create and make available an e-course for EAs across Europe; and e) disseminate and communicate the project results, activities, outputs and outcomes to key stakeholders.

In addition to the 26 EU MS that participate in the European Commission's (EC) Justice Programme, the project aims to reach, as far as possible, EAs in four candidate MS (Albania, Montenegro, North Macedonia, Serbia), where the General Data Protection Regulation (GDPR) or equivalent legislation already applies, in order to contribute to the integration process and to benefit professionals in these countries with limited access to transnational training opportunities.

PACE is implemented by the Centre for European Constitutional Law (CECL), as project coordinator, in partnership with the International Union of Enforcement Agents (UIHJ).

CECL is a leading research institute based in Greece, with a focus on the areas of Justice and democratic institutions, fundamental rights, rule of law and the welfare state. It is the National Focal Point of the Fundamental Rights Network (FRANET), of the European Union Agency for Fundamental Rights (FRA) and participates with two members in the composition of the Greek NHRI.

Founded in 1952, the purpose of the UIHJ is to represent its members in international organisations and to ensure cooperation with national professional bodies. The UIHJ works to improve national procedural laws and international treaties and seeks to promote ideas, projects and initiatives that help to advance and enhance the status of enforcement agents. In addition, the UIHJ participates in the structural actions of enforcement agents, in particular through its involvement in the creation and development of national professional organisations. It participates in investigative missions to governments and international bodies. Lastly, it promotes, wherever possible, the creation of a body of enforcement agents composed of professionals and senior legal officers who perform the role of officer responsible for both the service of judicial and extrajudicial documents and the enforcement of orders. The UIHJ has 100 member

countries. The UIHJ is a member of UNCITRAL and the Economic and Social Committee of the United Nations and has observer status in the CEPEJ (Commission for the Efficiency of Justice) of the Council of Europe. The UIHJ was a founding member of the European Law Institute (ELI). Wherever possible, the UIHJ is actively involved in strengthening the rule of law, promoting the judicial profession and offering its expertise in judicial reform. Since 2000, 50 UIHJ experts have participated in more than 200 projects organised and financed by European or international organisations or institutions (including the European Union, USAID, World Bank, IMF), ministries of justice, universities or professional organisations in more than 50 countries in Europe, Africa, America and Asia. It participates in expert missions close to governments and international organisations.

The project builds on the partners' previous work in the *ENABLE* and *EU enforcement Atlas* projects, that dealt with dematerialized access to information for the judicial enforcement of claims, and the mapping of enforcement procedures and practices in the EU MS, respectively.

Deliverable description. This document is *Project Deliverable D2.1 - TNA Report*. Its purpose is to capture the needs of EAs in Europe in relation to the application of the GDPR, in order to provide a sound evidence base for the development of a targeted, practical and relevant training programme.

Training Needs Assessment methodology. The Training Needs Assessment (TNA) is based on research and data collection carried out by the project partners with the support of national Chambers/Enforcement Authorities.

The research aimed to provide an overview of:

(a) The existing legal framework, practices and procedures relating to data protection in civil enforcement;

(b) Available tools and resources at national and EU level;

(c) Challenges and barriers for Enforcement Agents in the application of the EU data protection framework;

(d) the general level of knowledge of Enforcement Agents in relation to data protection and the extent to which they apply appropriate measures in their daily work;

(e) Specific challenges related to cross-border enforcement and enforcement in a digital environment.

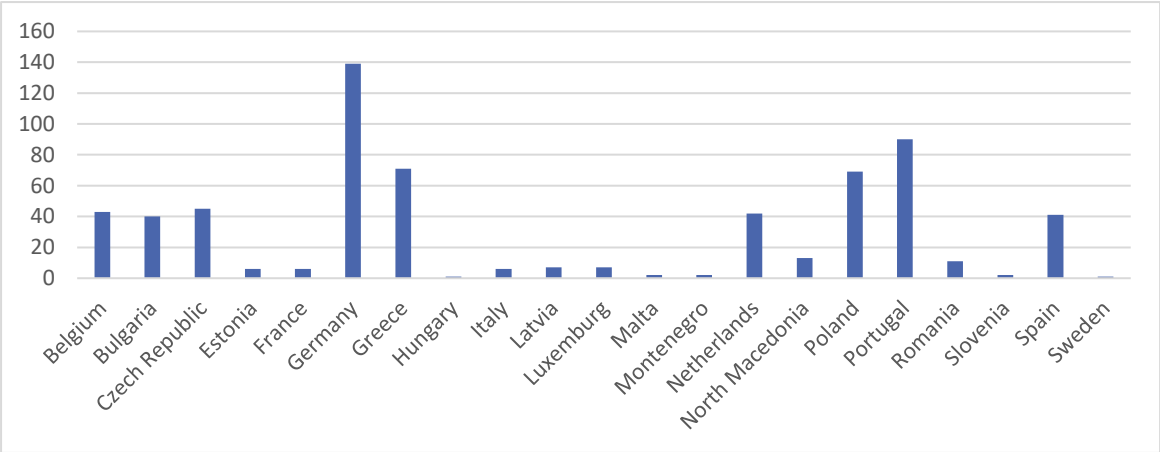
The partners identified gaps and bottlenecks, focusing on the common needs of EAs in the 24 EU Member States that participated in the PACE research, in order to give guidance on appropriate training approaches.

The TNA followed the participatory method and directly involved the target group at all stages. It comprised an online survey and in-depth interviews with key informants.

The online survey was the first part of our research, which aimed to provide quantitative insights into the level of knowledge and skills, as well as practices, of EAs in relation to the application of the GDPR. It was translated from English into national languages and disseminated through national Chambers/Enforcement Authorities to ensure representative results, regardless of language barriers. The survey received a total of 644 responses (383 male, 259 female, 3 preferred not to answer) from 23 EU Member States and 3 Candidate MS (Albania, Montenegro and North Macedonia), significantly exceeding the indicator of 180 participants set in the project proposal. Details on the number of participants per country are shown in Graph 1 below.

To complement the quantitative data from the survey with qualitative insights into the training needs of EAs, we conducted 24 in-depth interviews with key informants nominated by the Chambers/Enforcement Authorities of 21 EU Member States and 3 Candidate Countries (Albania, Montenegro and North Macedonia). The interviews aimed to identify institutional gaps, in particular those related to the support provided to EAs in their efforts to perform their tasks in compliance with the EU data protection framework, including guidance and tools, approved codes of conduct, training opportunities and individual assistance.

The questionnaires for the survey and the interviews are attached at the end of the document.



Graph 1 Number of responses to the online survey per country

Deviations. The deliverable was submitted with a delay of three months, due to difficulties in reaching the target group. The EU Member States Finland, Ireland and Slovakia and the EU Candidate Country Serbia did not respond to our requests. The project has made numerous requests by phone, email and through their known channels, but unfortunately has not been able to persuade the EA organisations in these countries to cooperate. The three EU Member States represent different enforcement systems: state enforcement (Finland), private enforcement (Slovakia) and court-based enforcement (Ireland). As these different systems are already represented among the respondents to our survey, we believe that the TNA still provides representative results that are relevant to EAs across Europe.

The GDPR and its significance to the work of Enforcement Agents

The GDPR entered into force on May 25, 2018. It represents a pivotal legal change that has not only reshaped the data protection landscape within the EU but has also influenced global conversations surrounding privacy in the digital era, impacting the way professionals operate across the board. Its main objectives include empowering EU citizens to control their personal data, strengthening data security measures and harmonising data protection laws across EU MS. At its core, the GDPR is characterised by a web of principles and provisions that collectively redefine data protection in the EU. Some of its key features include:

- **Territorial scope.** The GDPR extends its jurisdiction not only to organisations located in the EU, but also to organisations located outside the EU that process the personal data of EU residents. This reach ensures that the privacy of EU citizens is protected, regardless of the geographical location of the data processing. It also means that the GDPR is relevant to professionals and businesses beyond the EU and the European Economic Area.

- **Rights-based approach.** At the heart of the GDPR is a set of individual rights and corresponding guiding principles, including the lawfulness, fairness and transparency of processing, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability. These principles are implemented through a concrete set of safeguards, allowing individuals to have control over their personal data. In addition, the GDPR has driven a cultural shift in the professional world, with data protection compliance becoming a distinct priority.

- **Oversight and compliance.** The GDPR establishes a rigorous system of supervision and enforcement of its provisions. This is achieved through the appointment of Data Protection Officers (DPOs) at the level of individual organisations, Data Protection Authorities (DPAs) at national level and the European Data Protection Board (EDPB) at EU level. To further ensure compliance, the GDPR provides for sanctions for breaches of its provisions, including administrative fines of up to €20 million or up to 4% of an organisation's global annual turnover, in serious cases.

Under the GDPR, EAs are subject to concrete obligations in relation to the treatment of the personal data they collect and process in the course of their work, concerning, among others, the grounds on which they are processing the data, the extent of the processing and the categories of data processed and the length of their retention, the security of the

processing and the safety of the data they have stored in their archives. In addition, they must provide debtors with information and facilitate the exercise of their rights, while they are also often called to communicate with third parties, such as family members and other professionals. Where they operate beyond EU borders, EAs must comply with the GDPR's rules on international data transfers.

The significance of the GDPR for the work of EAs and the observed gaps in their relevant knowledge, five years after its entry into force, create the need for a targeted, relevant and practical training programme that will enable them to feel confident that they are performing their duties in compliance with the relevant framework.

Primary research findings: institutional background

Applicability of the GDPR

Since its entry into force in 2018, the GDPR has been applicable in all EU MS. In addition, the three candidate MS that participated in the PACE research, Albania, Montenegro, and North Macedonia, also apply data protection legislation that corresponds to and largely mirrors the provisions of the GDPR. The responses provided by the research participants indicate that they are aware of the data protection framework and the fact that it creates concrete obligations in relation to their work.

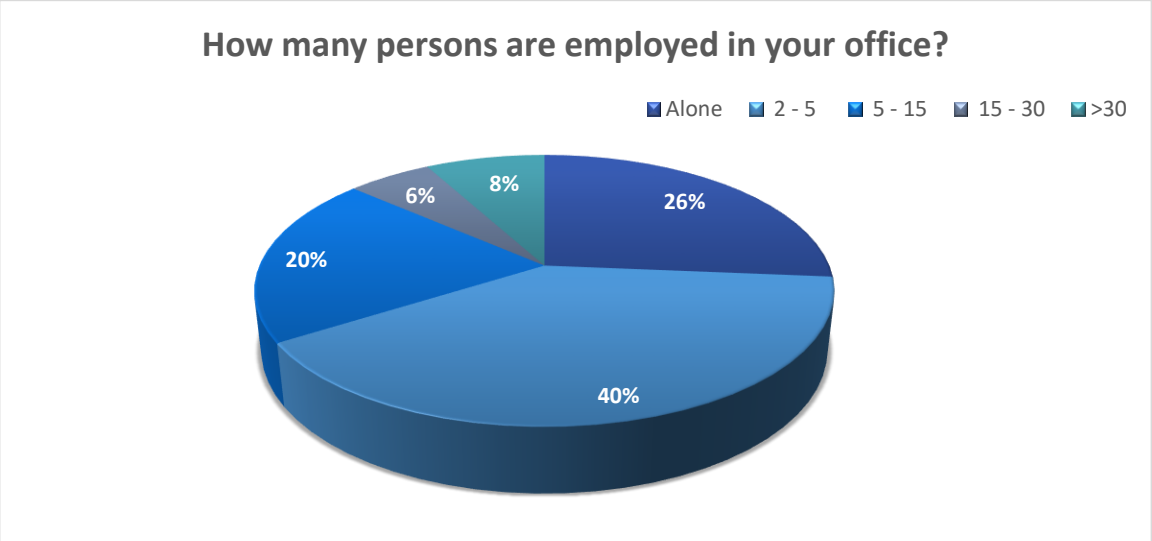
Structure of civil enforcement systems

It is important to note at the beginning of this chapter that the way in which the GDPR is applied, the specific obligations it creates for EAs, and the depth in which their training needs go largely depend on the way in which civil enforcement is organised in each MS or candidate MS. For an in-depth look into the features and particularities of the different enforcement systems in Europe, please visit the EU Enforcement Atlas website.

In some countries enforcement is performed by public bodies (e.g., Sweden) or administered by the courts' internal services (e.g., Italy), while in other countries it is carried out by private, self-employed professionals (e.g., Estonia) or there is a dual system where some enforcement activities are carried out by private bodies and others by public ones (e.g., Cyprus). In countries where enforcement is carried out by public officials, respondents reported that many of the privacy and data protection safeguards envisaged by the GDPR, including data protection by design and by default, retention periods, and the exercise of the rights of data subjects, are implemented by the competent authority, and EAs do not need to be concerned with the details of the relevant framework.

In contrast, in countries where enforcement is carried out by private practitioners, respondents rated knowledge of the GDPR as particularly important, since they are responsible for implementing all the relevant measures and also bear the full brunt of non-compliance. Even within this group of countries, however, we observed considerable differences, depending on the internal organisation of the relevant market. For example, in countries where enforcement services are provided by larger companies, respondents reported that the GDPR may be less relevant for the average Enforcement Agent, as many of the actions they have to take are regulated by office policy or handled by DPOs (e.g., the Netherlands). However, in countries where EAs tend to work in small offices or even individually, respondents were adamant about the importance of the GDPR in their daily work (e.g., Bulgaria).

This division is clearly reflected in the responses research participants gave when asked to reflect on the relevance of the GDPR to their work. Specifically, although the majority of interviewees indicated that the GDPR is important, many were clear in mentioning that the degree of relevance depends also on the position of the EA within the enforcement office/agency.



Graph 2 Number of persons employed in a single civil enforcement office or agency

The graph above shows that the majority of respondents to the online survey (66%) work in micro practices, employing 1-5 persons. Moreover, 41% of all respondents reported not having or being unsure if they have access to a DPO.

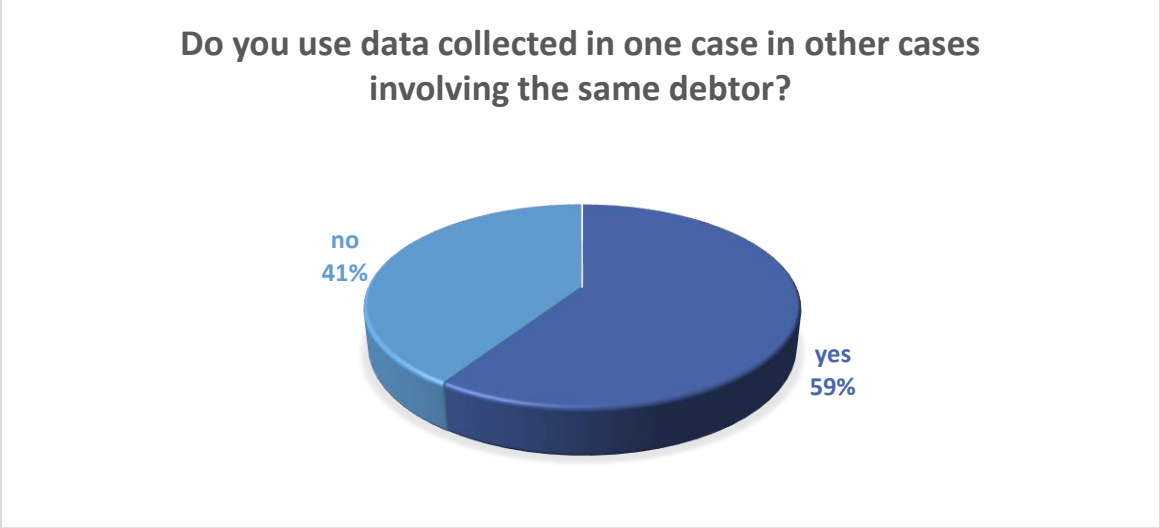
Relevance of the GDPR and main areas of concern

Respondents report a variety of areas of their work to which the GDPR is relevant. Again, the degree of perceived or actual relevance depends on the system in which their work is organised (public/private, etc.). Regarding specific enforcement acts, respondents mentioned in particular evictions and the service of documents, whereas they were also concerned about the handling of cases where the debtor is vulnerable.

As far as data processing acts are concerned, a prominent example mentioned by many respondents is the protection of the debtor's privacy during enforcement acts. This includes the measures that the EA is obliged to have in place to protect the debtor's identity, which may be visible on enforcement documents, envelopes, etc. (e.g., covering the debtor's name and contact details); addressing correspondence, including paper and digital, in an appropriate and secure manner; communication with third parties who may be present during acts of enforcement, including family members requesting information,

or other professionals involved in the enforcement, such as locksmiths assisting in evictions.

Respondents were also concerned about the lawful processing of a debtor's data available from other sources, particularly in relation to the principles of purpose limitation and data minimisation. This includes data available to the EA from other cases against the same debtor that their office may be handling, as well as data available through public databases (e.g., in Sweden, information on bank debts is publicly available). The graph below shows the importance of this particular issue, with more than half of the respondents to the online survey reporting that they do use data collected in the context of other cases.



Graph 3 Percentage of EAs that use debtors' data collected for other cases

Last but not least, an important issue highlighted by many respondents is the management and organisation of their case files in accordance with the safeguards envisaged by the GDPR. This concerns both physical and digital archives. Gaps and needs related to digital information security, readiness and data protection by design and by default are addressed in the section regarding implemented safeguards. It is important to note that the majority of respondents report using predominantly digital means to store, process and transfer debtors' personal data (52% of respondents to the online survey report using digital means 90-100% of the time, 76% report using digital means 70-100% of the time), while only 10% use digital means less than 50% of the time. However, a non-negligible percentage of EAs within the respondent countries report a use of digital means below 50% (notably, 50% of respondents in Italy, 23% in Greece, 19% in Poland, 18% in Romania and Portugal).

A related issue, addressed below under practical, legal and policy barriers, is confusion about retention periods and the often conflicting relevant provisions of national law. Many respondents report feeling overwhelmed by the need to balance their obligations to limit processing under the data protection framework with their various other legal obligations under national law.

Practical, legal, and policy concerns

Respondents generally expressed uncertainty about how to comply with all the obligations arising from the GDPR and relevant national frameworks, while at the same time effectively and transparently enforcing civil law claims. This is particularly evident in nuanced cases, such as those where the data subject themselves have made some of their personal data in question publicly available. A lack of clear understanding of the principles of data minimisation and purpose limitation seems to be a maEAr concern in this respect. At the same time, EAs also reported feeling insecure when debtors use privacy and data protection objections as a means to delay the enforcement of claims against them. These sentiments point to the need for training on the basic notions and principles tied to the GDPR, so that EAs can feel confident that they are performing their duties in accordance with the relevant framework and can reject unfounded objections from debtors, as well as other persons involved in civil enforcement (e.g., public officials). Indeed, the lack of systematic training and clear, step-by-step guidance on the application of the GDPR was identified by respondents as a clear challenge they face.

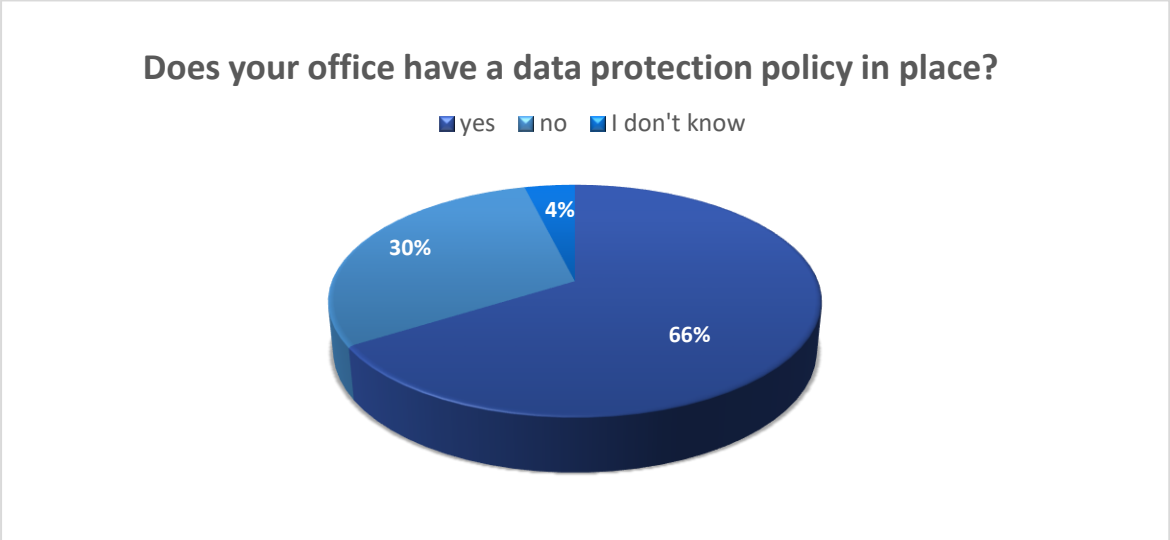
Another practical issue raised by interviewees is the significant organisational and administrative burden associated with ensuring that enforcement bodies operate in a GDPR-compliant manner, including upfront costs such as legal/Data Protection Officer fees, costs associated with the implementation of technical/organisational measures, etc.

Next, respondents highlighted bottlenecks in communication and interconnection between the different bodies involved in civil enforcement, including courts and public authorities. In particular, respondents reported that public authorities are often reluctant to share information necessary for the EA to carry out its work because they are overly cautious or mistakenly believe that they have a legal obligation not to share the data without the data subject's consent. On the other hand, the use of data made available through public databases is also a source of concern, in particular with regard to the regulation of the interconnection of different public databases and the use of data in accordance with the purpose limitation principle. Thus, EAs are often called upon to deal with situations where either too little or too much personal data is made available to them by other public authorities.

Several respondents also pointed to gaps and inconsistencies in the legal and regulatory frameworks of their MS, which give rise to concerns, in particular with regard to retention periods and the sharing of data with third parties. Some of the concerns expressed in this respect are listed below. In Germany, the respondent highlighted the problem of resale of data collected by EAs to third parties - a problem they try to prevent by including relevant notices in all enforcement documents. In Greece, different laws on retention periods often contradict each other, causing confusion both for EAs as to their specific obligations and for other legal professionals involved in the enforcement process. In particular, the Greek respondent mentioned that prosecutors have often prevented EAs from deleting files after the expiry of the retention period provided for in the law implementing the GDPR. The Luxembourg respondent reported that the framework requiring a 30-year retention period is still applicable, which creates conflicts with key principles and provisions of the GDPR. The Maltese respondent mentioned that there is no framework for retention periods in civil cases. In the Netherlands, the KBvG (Royal Professional Organisation of Enforcement Agents) is critical of the insufficient protection of the debtor's privacy in the case of third party wage garnishment. In particular, they criticise the fact that the details of each claim, including the cause of the debt (e.g., gambling), are communicated to the debtor's employer. Civil procedure in Poland creates a risk that enforcement proceedings may be initiated against a person who is not the debtor (although this risk has decreased following recent reforms), and thus there is a risk that the personal data of third parties may be processed without a legal ground.

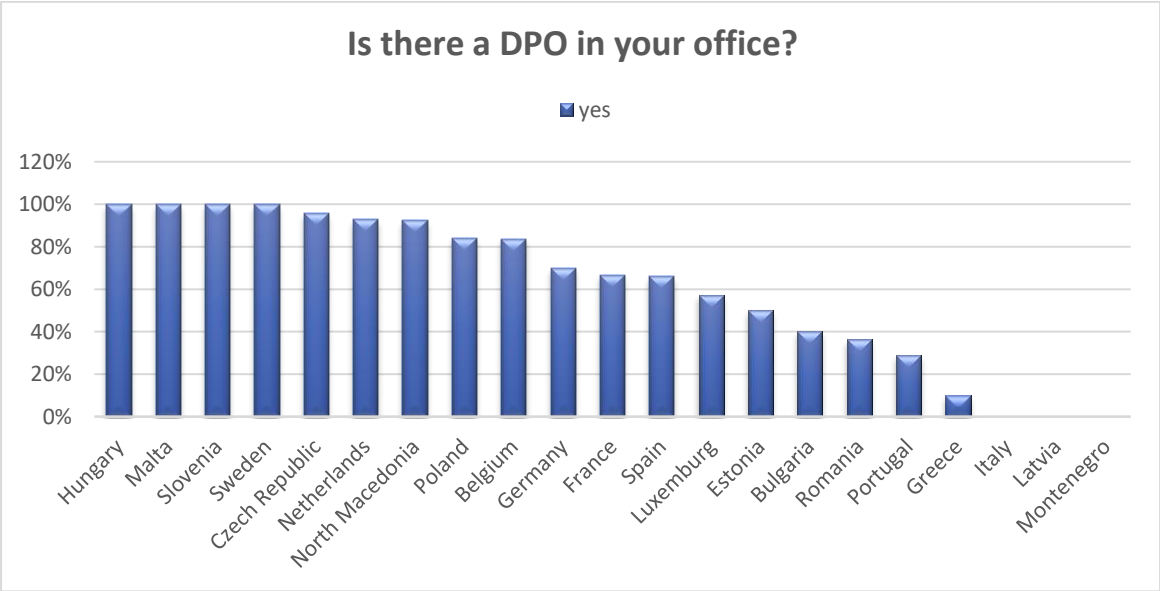
Implemented safeguards

Next, the TNA sought to capture the most common safeguards already implemented in the participants' offices. The first step to ensure GDPR compliance is the existence of a comprehensive data protection policy. In this respect, 66% of respondents indicated that their office does indeed have a data protection policy in place, albeit with large differences between Member States. Indicatively, more than 90% of respondents from Germany indicated that their office did not have such a policy, while respondents from other countries (e.g., Estonia, Greece, Romania) were almost equally divided in their answers to this question. At the same time, the existence of a data protection policy is only an indicator of compliance, as the content and comprehensiveness of each individual policy are not assessed in the context of this research.

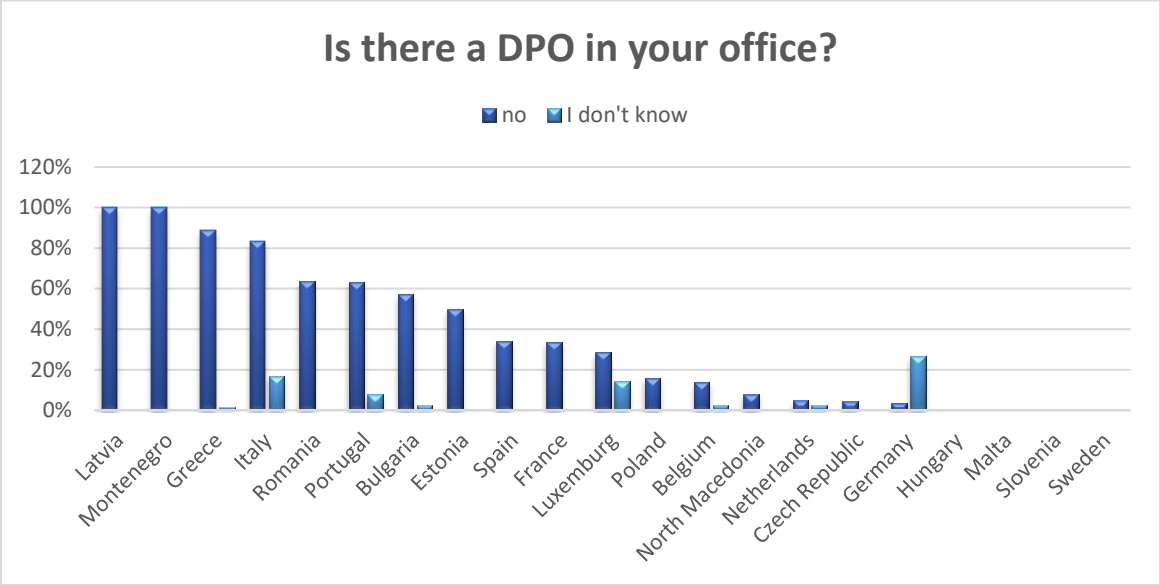


Graph 4 Percentage of offices with a data protection policy

Another such indicator is the presence of a DPO working with civil enforcement authorities, either as an internal or external expert. As the GDPR requires a certain level of expertise and assigns specific responsibilities to DPOs, this is a safer way to assess overall compliance. In this respect, 59% of respondents answered in the affirmative, although again with wide variations across the participating countries, as shown in Graph 4.



Graph 5 Percentage of offices with DPOs per country



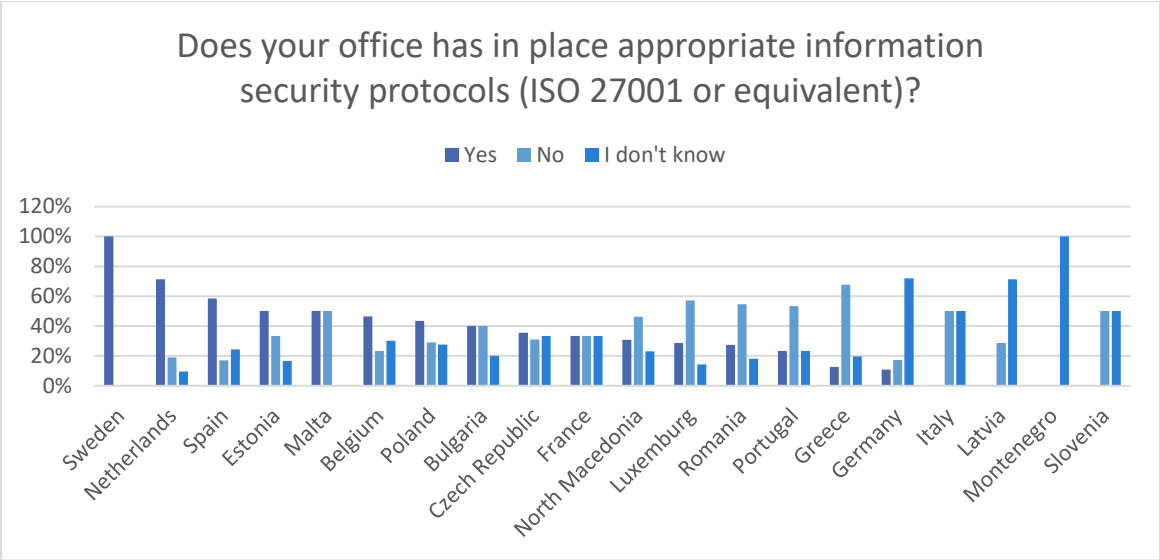
Graph 6 Percentage of offices without DPOs per country

Despite the differences in the degree of digitalisation of civil enforcement in the MS and candidate countries, digital enforcement as a whole is steadily gaining ground. In addition, as mentioned above, the vast majority of EAs use some form of digital storage system, send data related to enforcement cases, including potentially personal data of debtors, by e-mail and use cloud storage for at least part of their files. In addition to information security measures aimed at ensuring data protection by design and default, the use of digital tools to process personal data also requires appropriate training and awareness of the staff involved in the processing activities. However, a clear majority of respondents report that they are either not aware of or do not have appropriate information security protocols (ISO 27001 or equivalent) in place to ensure that data is transferred and processed securely.

In addition, the vast majority of respondents to the online survey (89%) reported that they personally have access to all information stored in their office's files, including personal information about debtors. However, 79% reported that their office has at least some technical/organisational measures in place, including personal passwords/IDs and measures to restrict physical access to files, such as locks, to limit who can access what type of data. In addition, 70% of respondents claim that external service providers and affiliates, such as IT support, cleaning services, etc., do not have access to data stored in their offices (25% claim that they do, while 5% do not know). This apparent contradiction indicates a lack of awareness of the operation of technical and organisational measures in the context of data protection and calls into question the effectiveness of the measures in place to prevent unauthorised access to all files. For example, a lack of awareness that

the password on one's own computer is used to protect not only one's own personal data but also the personal data of others stored there may allow inappropriate sharing of data between staff (e.g., sharing of data from other cases against the same debtor, shown to be a maEAr source of concern in Graph 2).

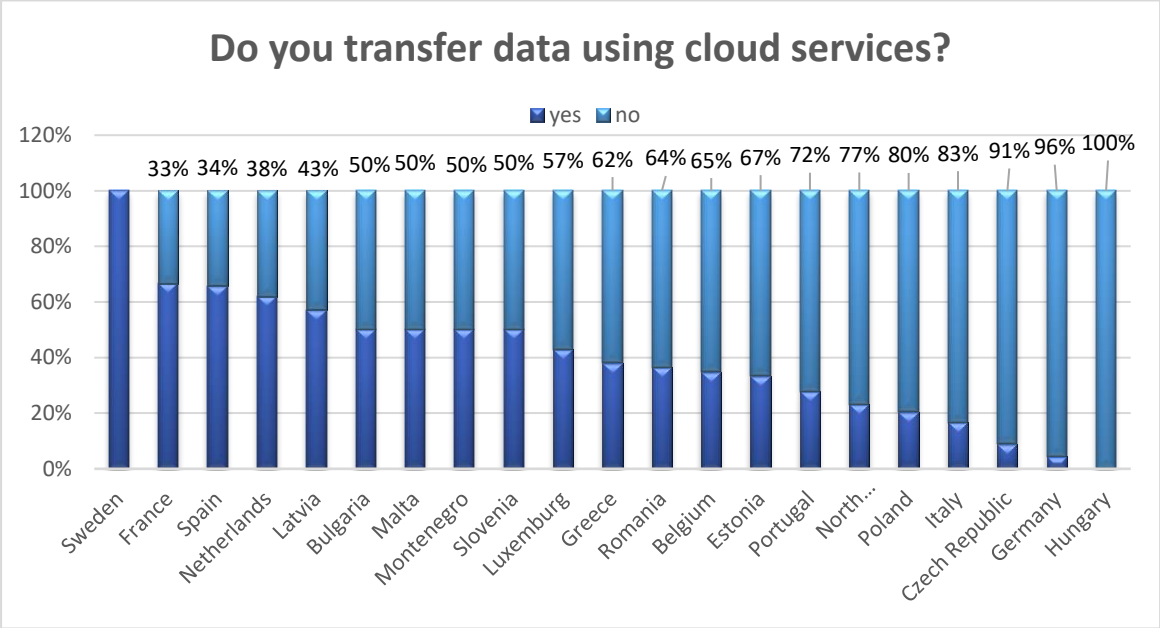
The graph below shows the percentage of offices with information security protocols in place per participating country. Note that in Sweden, enforcement is carried out by a single public authority.



Graph 7 Existence of information security protocols per country

Another key issue explored in the PACE research is the awareness and readiness of EAs to respond to the challenges of cross-border data protection enforcement, particularly in relation to the transfer and processing of data in third countries. It should be noted that respondents rated the relevance of this particular issue to their daily work as very low, with 93% reporting that less than 5% of their cases involved the transfer of data to third countries. In addition, 67% reported that they do not apply any safeguards when processing data in third countries, including not checking for the existence of adequacy decisions issued by the EC or any other safeguards provided for in Chapter V of the GDPR.

A significant percentage, varying from country to country, also reported using cloud services in their daily work. Combined with the figures above, this may indicate a lack of awareness that cloud storage and processing may involve processing in a third country and therefore require action by the EA to ensure that an equivalent level of protection is guaranteed in accordance with Chapter V.



Graph 8 Percentage of EAs using cloud services per country

Guidance and support provided by Chambers and enforcement Agencies

Chambers and Enforcement Agencies support their members by:

- Issuing general guidance and instructions on the application of the GDPR;
- Organising training activities on privacy and data protection for their members; and
- Providing individual guidance to EAs on how to apply the GDPR in their daily work.

In terms of general guidance, instructions and tools, interviewees were divided, with around half of them (10/24) indicating that there are no official instructions provided centrally to EAs to help them respond to the challenges posed by the GDPR in a consistent manner. In the remaining countries (12/24), either the Chamber or other competent authorities (courts, MoJ) have issued such instructions, which are generally considered to be of at least adequate quality. However, it was noted that these guidelines and instructions need to be updated to reflect developments that have occurred between the entry into force of the GDPR and the present day.

The guidelines and instructions may occasionally take the form of a code of conduct, in accordance with Art. 40 GDPR. To date, only two national Chambers have adopted such codes: the Bulgarian and the Portuguese ones. In addition, the Royal Professional Organisation of Enforcement Agents in the Netherlands has prepared a Code of Conduct,

pending approval by the Dutch DPA, whereas the preparation of a Code is also underway in Hungary.

With the exception of the Czech Republic and Luxembourg, where there is no central authority or body responsible for the training of EAs, but all training is left to the individual initiative of the EA to identify private training opportunities, all other countries have some system in place to ensure that training opportunities tailored to and targeting EAs are available. In most cases, the national and/or local chambers are responsible for organising training activities on various topics relevant to EAs, often alongside other agencies and the Ministries of Justice. In countries where enforcement is administered by public agencies, the agency is responsible and organises regular training for its staff.

In most countries there is a mix of public and private training opportunities for EAs. It should be noted, however, that most respondents highlighted the lack of emphasis on the topic of data protection. Notable exceptions to this trend are Belgium, Hungary, Lithuania, the Netherlands, Portugal, and Romania. Respondents from these countries mentioned that trainings on the GDPR are organised regularly (approximately once a year).

Finally, as regards individualised support and advice to EAs on the practical application of the GDPR, most chambers do not provide that, with the notable exception of countries where enforcement is administered by a public authority (e.g., Sweden). In countries where enforcement is privately administered, large enforcement bodies often have DPOs (internal or external) who can act in this capacity and assist individual EAs with their day-to-day tasks.

Complaints and disciplinary proceedings

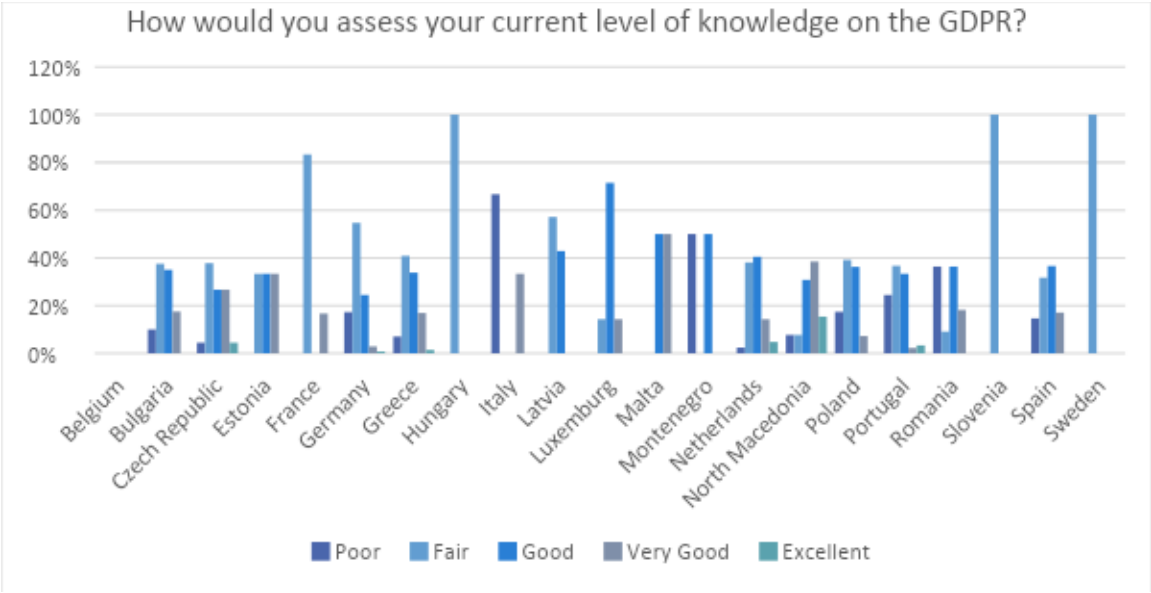
Most Chambers and Enforcement Agencies are competent to receive complaints about data breaches by EAs in the context of enforcement. No data were available on the average number of such complaints, but respondents reported that they very rarely, if ever, resulted in disciplinary proceedings against EAs.

Training needs

As the above analysis shows, there are significant differences between PACE beneficiary countries in the way they organise their civil enforcement systems, which has a significant impact on the type of training that is relevant to the work of enforcement officers in each country. A key finding of our research is that in countries with a state or court-based enforcement system (i.e., in countries where enforcement is assigned to a state agency or carried out directly by the courts), a large part of GDPR-related obligations is handled at the central level, either by a small group of specialised EAs or by the administration of the relevant body, often in cooperation with internal or external DPOs. In this case, a large part of the GDPR, especially as regards technical and organisational measures, is not particularly relevant for the average EA in these countries. On the other hand, in countries with private enforcement systems, even if a DPO is established in the authority, the GDPR remains relevant for the vast majority of EAs, who are individually responsible for ensuring that they carry out their work in a GDPR-compliant manner. With this in mind, and in order to provide the maximum added value to the larger number of participants, the PACE training offer should primarily address the needs of private EAs.

Enforcement Agents

Data from our research suggests that EAs rate their own knowledge of the GDPR poorly. Specifically, the majority of respondents to the PACE survey (55%) rate it as poor or fair, 32% as good and only 13% as very good or excellent. There are significant differences between countries, as shown in Figure 8 below.



Graph 9 Self-assessment of overall knowledge of the Graph 2 of the GDPR per country

The findings analysed above identify a number of topics where a lack of knowledge is evident. These include key concepts and principles, as well as very practical measures required to ensure compliance with the GDPR. In particular, respondents highlighted

- Managing their filing system;
- Compliance with the legal and regulatory framework on retention periods;
- Applying the principles of data minimisation and purpose limitation;
- Data sharing with third parties;
- Dealing with challenges related to the behaviour and perceptions of other justice professionals and competent authorities.

In addition, it is clear that training is also needed to address gaps in information security in a digital environment and in the transfer of data to third countries.

Self-reported levels of knowledge, as well as responses to questions designed to test knowledge, suggest that a significant majority of EAs are in need of initial training, which should be emphasised in PACE training activities.

In terms of their preferred training methodology, all participants emphasised their desire for step-by-step practical guidance on how to carry out their daily tasks, rather than theoretical knowledge.

Trainers

The PACE research shows that there is a notable lack of EAs trained to act as trainers for their peers, in particular on the topic of data protection. While Austria stands out as an exception, with a relatively robust infrastructure for GDPR training, many other European countries face a shortage of qualified trainers in this crucial area. This imbalance in training resources poses a significant challenge to ensuring that EAs across Europe are equipped with the knowledge and skills necessary to effectively navigate the complex legal landscape of the GDPR, leaving a significant gap in the implementation and enforcement of data protection rules.

Training suggestions

Training methodology. Bringing together civil enforcement and data protection in a single training offering poses significant and unique challenges. The structure of different enforcement systems, the different responsibilities of EAs within them and the different qualifications required to enter the enforcement profession all contribute to significant difficulties in identifying competent trainers, interested trainees and relevant training topics.

In order to address the above challenges, the training should follow a participatory approach, drawing on the trainees' experience in civil enforcement and addressing the privacy and data protection issues they face in their daily work. Problem-based exercises, building on their own experience, should help to create a relevant and practical programme. The topics identified in the TNA should serve as a basis for the development of the PACE training package. However, the package should be enriched by input from the train-the-trainer workshops, where additional issues and gaps may emerge.

To this end, the ToTs in particular should emphasise interaction and promote the exchange of knowledge and experience between trainers and trainees. The training should focus on practical understanding of the GDPR, but also include didactic elements to help participants acquire the skills and competences to deliver effective training to their peers.

Trainee profile. The proposed methodology of selecting participants in cooperation with the relevant Chamber/Enforcement Authority is well suited to compensate for the observed diversity of enforcement systems and to help the project identify the trainees who would most benefit from its offer. As mentioned above, our research shows that the average level of knowledge of the EU data protection framework among EAs is poor to fair, suggesting that a focus on initial training would most benefit a clear majority of European EAs. The selection of participants should aim to identify EAs with a basic level of knowledge of the GDPR.

In addition, the PACE training offer should be more tailored to the needs of private EAs, for whom the obligations imposed by the GDPR are more relevant. This may mean that countries with a state or court-based enforcement system may be underrepresented in some of the webinars. However, we propose that the project draws on the expertise of specialised EAs in these systems, who are knowledgeable about both data protection and the day-to-day challenges of enforcement, and who could be excellent participants in the train-the-trainer workshops. The selection of participants for the ToTs will be crucial, as the trainers trained there can bridge the gap between GDPR expertise and knowledge of enforcement. This will add maximum value to the webinars delivered with the help of these trainers, but will also help to further build the capacity of enforcement authorities to provide peer learning based training opportunities.

However, in order to also help chambers in private enforcement systems build the much-needed capacity to provide GDPR training to their members, ToT participants should represent all systems. Non-specialist participants should preferably have experience in delivering training to other legal professionals, in particular EAs. As the ToTs will be

delivered in English, a working knowledge of this language should be included in the selection criteria.

Trainer profile. The ideal trainer for the PACE training programme is someone who can bring together the worlds of civil enforcement and data protection. However, our research has shown that this is a significant challenge. Indeed, identifying legal professionals who are both GDPR experts and familiar with the inner workings of civil enforcement is a demanding task. To compensate for this, more trainers with complementary expertise should be selected.

Trainers should be experienced in delivering training to legal professionals, ideally including EAs, and have an excellent working knowledge of English.

ANNEX 1 Online Survey questionnaire

Survey Title: PACE SURVEY FOR JUDICIAL OFFICERS

Brief for participants: The International Union of Judicial Officers (Union Internationale des Huissiers de Justice) invites you to participate in this online survey, which aims to record your current capacities and needs in relation to the application of the EU data protection framework (GDPR) in your line of work. The survey is part of the activities of the EU-funded project titled *Creating Privacy awareness in civil enforcement – PACE* (101090018 — PACE — JUST-2022-JTRA).

The estimated time to compete the survey is 10-15 minutes. Please respond to all questions.

Thank you for your input!

Survey Questions

1. In which country do you ordinarily perform your duties?

   [dropdown list of 26 EU MS – minus Denmark - +4 Candidate MS - Serbia, North Macedonia, Albania and Montenegro]

2. What gender do you identify as?

   a) Male

   b) Female

   c) Other

   d) Prefer not to say

3. How many persons are employed in your office?

   a) I work alone

   b) 2-5

   c) 5-15

   d) 15-30

   e) >30

4. How would you assess your current level of knowledge on the GDPR?

   a) Poor

   b) Fair

c) Good

d) Very good

e) Excellent

5. Does your office have a data protection policy in place?

a) Yes

b) No

c) I don't know

6. Has your national Chamber of Judicial Officers adopted a Code of Conduct on data protection, to which you must comply when exercising your duties?

a) Yes

b) No

c) I don't know

7. Do you have a DPO within your office who is responsible to ensure compliance with the GDPR and whom you can consult on data protection-related issues?

a) Yes

b) No

c) I don't know

8. At what percentage do you use digital means to store/process/transfer the data you collect (including a computer, server, storage devices, digital cloud)?

a) <30%

b) 30-50%

c) 50-70%

d) 70-90%

e) >90%

9. Does your office have in place any information security protocols to ensure that data processed digitally are secure (e.g., ISO 27001 standards or equivalent)?

a) Yes

b) No

c) I don't know

10. Do you, personally, have access to all the data stored in your office file system/server?

    a) Yes

    b) No

11. Do you, personally, use data collected in the context of one case in other cases involving the same natural person(s)?

    a) Yes

    b) No

12. Does your office apply a traceability system within its network in order to track which staff members accessed which documents?

    a) Yes

    b) No

    c) I don't know

13. Does your office have in place a system that limits who can access which type or groups of data within your office (e.g., password protection, use of personal IDs, physical barriers, such as locks, etc.)?

    a) Yes

    b) No

    c) I don't know

14. To your knowledge, do external service providers or affiliates have access to the data stored in your office (e.g., IT technicians, cleaners, other)?

    a) Yes

    b) No

    c) I don't know

15. What percentage of your work involves the transferring of data to and from non-EU countries?

    a) <5%

    b) 5-20%

c) 20-35%

d) 35-50%

e) >50%

16. Do you transfer data using cloud services?

a) Yes

b) No

17. When transferring data to and from non-EU countries, including through the use of cloud services, what information do you check to ensure the processing of data is performed lawfully (select all which may apply)?

a) The existence of relevant European Commission decisions (adequacy decisions)?

b) The existence of binding corporate rules applicable by the processor, ensuring an adequate level of protection?

c) The incorporation of standard contractual clauses on data protection into your contract with the processor?

d) The display of a Certification logo on the processor's website?

e) The existence of an approved code of conduct?

f) None of the above?

18. Have you received any formal training on the application of the GDPR?

a) Yes

b) No

19. How often do you participate in training activities related to the GDPR?

a) Once a year

b) Once every two years

c) I have been trained once on the GDPR

d) I have never received training on the GDPR

20. Do you have at your disposal guidelines, material, or tools to help you ensure privacy and data protection in accordance with the GDPR in your work?

a) Yes

b) No

21. How would you assess their quality/usefulness/practicality?
    a) Poor
    b) Fair
    c) Good
    d) Very good
    e) Excellent
22. Would you like to share any insights, observations or wishes on what you personally would like to see in a training on the GDPR for judicial officers (e.g., on the training methods used, the orientation of the training – practical vs theoretical, the types of training material you would like to receive, etc.)

ANNEX 2 Interview questionnaire

Interview Questionnaire

Interviewee code: I01, I02, I03, etc.

Interviewer: [name, surname, capacity, organisation]

Interview date:

Location:

The interviewee has been informed about the purposes of the research and the processing of their personal data, and has provided consent to participate □

The interviewee withdrew their consent during the interview □

Introductory questions

Country	
Chamber	
Capacity within the Chamber	
Other affiliated entity (if Chamber N/A)	
Gender	

Operational needs/gaps

Is the GDPR applicable in your State's legal order (relevant for candidate MS)? If not, how would you assess its influence to your data protection legal,	

policy and practical framework?	
Is knowledge of the GDPR important in the work of a judicial officer?	
To which thematic areas of a judicial officer's work is the GDPR more relevant?	
What would you say are the biggest challenges for judicial officers in their efforts to ensure privacy and data protection in civil enforcement? Are there any practical/policy barriers they need to overcome in practice?	
How would you assess the quality of the guidelines, tools, and regulations available to judicial officers in your country to help them execute their tasks in a manner compliant to the GDPR? How would you improve these?	
Is your Chamber responsible to provide guidance or consult judicial officers on data protection-related issues?	

Has your Chamber issued a code of conduct on data protection, in accordance with article 40 GDPR?	
How many complaints do you receive for data breaches related to the work of judicial officers of your Chamber (if applicable)? How many of these result in disciplinary cases?	

Training received/provided

Who is responsible for the training of judicial officers in your jurisdiction concerning data protection (Chamber of Judicial Officers, other private/public actors)?	
To your knowledge, how frequently are training activities on the GDPR organised for judicial officers within your jurisdiction?	If there is official data available on these figures, the interviewee should be asked to provide these, if possible
In your view, what are the key thematic areas within the line of your work on which data protection	

training for judicial officers should focus?	
Are judicial officers trained to respond to needs related with enforcement in a digital environment?	
Are judicial officers trained for cross-border/extraterritorial enforcement?	
How would you assess the quality of the above training in terms of its relevance to judicial officers, its practical impact and the methodologies used?	
Do you provide training to judicial officers within your chamber to become trainers on GDPR-related issues? How about on other topics?	Enter N/A if the organisation/Chamber in question does not provide training to judicial officers
In your assessment how many judicial officers within you chamber are capable of providing training to their peers/act as multipliers of GDPR-related knowledge and skills?	

What do you think is missing in terms of the training provided to judicial officers on the GDPR? How can such training be more effective in terms of addressing the needs related to the exercise of the judicial officers' duties?	

Concluding questions

Is there anything else you would like to add that was not covered in our discussion? Is there anything in particular you would like to see in the PACE trainings (in relation to training methodologies/material, etc.).	
Are there any specific resources/material on the topic of GDPR training that you have found relevant and useful and you are at liberty to share with us?	

Probes

The probe is simply a question or statement which encourages the interviewee to add to or elaborate on something which was said. Here are some examples of probes.

- Could you elaborate?
- Could you give an example?
- Could you explain this a little bit further?
- Would you like to add anything else?