SPARTA

D2.6

General guidelines for responsible cybersecurity research and innovation

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February, 2019
Duration	41 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D2.6 / V1.0
Work package contributing to the deliverable	WP2
Due date	June 2022 – M41
Actual submission date	14th September, 2022

Responsible organisation	Fraunhofer
Editor	Michael Friedewald
Dissemination level	PU
Revision	V1.0

Abstract	This deliverable presents the research on selected current emerging legal issues of relevance for researchers in cybersecurity. The issues are first data protection requirements in collaborative European research (especially in cybersecurity) and second the legal uncertainties connected with the co-ordinated disclosure of vulnerabilities.
Keywords	Cybersecurity, cybercrime, information systems, Coordinated vulnerability disclosure, criminal responsibility, protection, researcher

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

Editor

Michael Friedewald (Fraunhofer)

Contributors (ordered according to beneficiary numbers)

Manon Knockaert, Sophie Everarts de Velp, Jean-Marc Van Gyseghem (UNamur)

Regina Valutytė, Simas Grigonis (MRU)

Reviewers (ordered according to beneficiary numbers)

Volkmar Lotz (SAP)

Rocco De Nicola (CINI)

Executive Summary

This deliverable presents the research on two selected current emerging legal issues of relevance for researchers in cybersecurity.

The first part provides some general guidance for responsible and legally compliant cybersecurity research and innovation with its large amount of often personal data. It takes into account what the European Commission's objectives are for future collaborative research. In doing so, we analyse the interactions between research policy goals and data protection regulations and make suggestions on how to achieve a good balance between the two. We conclude that the General Data Protection Regulation allows for some adaptations to the specific situation of the use of personal data for scientific research purposes, especially those with high societal relevance, such as cyber security. The limiting factor here is that beyond the actual research process, the stricter general rules of data protection law must be observed, for example in the use of data that is not collected for research purposes or in the operation of the technical systems developed.

As a result of Directive (EU) 2019/1024 on open data and the re-use of public sector information, researchers must be prepared to make all data from publicly funded research available for re-use by third parties free of charge and in accordance with FAIR (findable, accessible, interoperable, re-usable) principles. Finally, the recently adopted Data Governance Act and the Data will create the possibility of altruistic data sharing to improve research for public interest purposes within the Union harmonized rules for fair access to and use of data.

The second part addresses issues connected to the "Coordinated (Controlled) Vulnerability Disclosure" (CVD) model requiring that a vulnerability be disclosed to the public only after the responsible parties have been allowed sufficient time to patch or remedy the vulnerability. For the time being, CVD takes place in a legal grey area where even actors with the best of intentions risk being prosecuted. The analysis of the legal regulations in the member states of the EU shows that CVD is not regulated in all countries, and that regulations differ significantly or are even contradictory. Thus, activities that are legal in one country may be illegal in another. It is argued that it would be useful to harmonize legal regulations in Europe so that CVD can take place under equal conditions and without the risk of criminal prosecution.

Table of Content

List of Figures

Chapter 1 Introduction

One of the goals of the "accountability activities" within the SPARTA project was to provide guidance to researchers and developers involved in cybersecurity research that goes beyond the specific problems and scope of the individual SPARTA programmes. Elements of this guidance have been presented in previous deliverables.

Previously in D2.1 [37], we have analysed the relevant legal aspects in the context of large-scale cybersecurity research and innovation after defining the cybersecurity notion. We focused on safeguarding fundamental rights in cybersecurity research and innovation. This choice was explained by the fact that security must serve the fundamental rights recognized by the European Union.

Then, in D2.3 [59], we presented the common issues identified among the SPARTA Programs concerning General data protection regulation (GDPR) compliance during the project's lifetime. During the meetings with the experts working in the SPARTA Programs, we identified some misinterpretations around the concept of protection of personal data and explained these related notions. The correct understanding of the key definitions of the GDPR is the prerequisite for the successful embedding of the data protection principles while developing a technological solution. We examined the exceptions to privacy laws in the context of national security, the category of national security itself and evolving practices. Our contribution reflected on the concept of the national security exemption established in GDPR. Moreover, we have reviewed the laws and strategies regarding national security that have been enacted by some selected Member States.

This deliverable now expands the scope of our previous work by addressing current and emerging issues.

Chapter 2 of this report provides some general guidance for responsible and legally compliant cybersecurity research and innovation. It takes into account what the European Commission's objectives are for future collaborative research. In doing so, we analyse what interactions there are between research policy goals on the one hand and data protection regulations on the other and make suggestions as to how a good balance between the two can be achieved. Of particular importance are the draft regulations currently being negotiated in the area of data use, i.e., artificial intelligence act, data act, data governance act and the recently adopted Digital Services Act and the Digital Markets Act.

Chapter 3 addresses issues of "Coordinated (Controlled) Vulnerability Disclosure" (CVD). The identification of cyber vulnerabilities in existing systems is an important area of cybersecurity activity, as their exploitation can lead to serious damage and disruption. However, there are also particular legal uncertainties associated with this, as the intrusion and analysis of systems and the disclosure of identified vulnerabilities are potentially criminal acts, even if performed with good intentions. So far, CVD is only regulated in some EU member states, and these regulations are not harmonised across Europe, with the result that practices that are legal in one country may be illegal in another. In the chapter we provide an overview of the regulatory landscape in Europe and discuss the need and added value of an EU-wide regulation that would exempt CVD from criminal liability.

Chapter 2 Data protection law in scientific research

2.1 Introduction - Concept of European scientific research

In every scientific research that includes personal data, a balance has to be found between a massive or excessive use of data for cybersecurity purposes and a legal framework for the protection of personal data that allows cybersecurity research. Thus, this chapter concludes the work on data protection issues by analysing the concept of European scientific research and the strategy developed by the European Union in this regard, as well as the impact of the GDPR on this subject. This chapter aims to demonstrate, through guidelines, that the protection of personal data strikes a balance between the protection of privacy and the need for scientific research.

2.1.1 European approach to research

Although there is no specific definition of the notion of European scientific research in the legislation, article 2, 1° of the Regulation of the European Parliament and of the Council of 11 December 2013 establishing the framework program for research and innovation "Horizon 2020" (2014-2020) and repealing Decision No 1982/2006/EC refers to the notion of research by defining the term "*research and innovation activities*" as " *the whole spectrum of activities of research, technological development, demonstration and innovation, including the promotion of cooperation with third countries and international organisations, the dissemination and optimisation of results and the stimulation of high quality training and mobility of researchers in the Union*".

Moreover, by analysing the common language to better understand what European scientific research meant, we were able to arrive at the following definition "*A set of studies and work carried out with rigour, high standards, objectivity, method and precision by a specialist with the aim of advancing knowledge at European level*"[1].

More concretely, the European Union is facing an increasing global competition in scientific and technological research and development [20]. For several years, strategies and investments have been put in place to address this problem. Recently, two framework programs have been implemented: Horizon 2020 (2014-2020) [7, 21] and Horizon Europe (2021-2027) [4]. It attempts to continue the objectives proposed by the Horizon 2020 program by focusing on three pillars: Science and Technology, Society, Economy. Open science is also a fundamental part of the strategy[2]. The European Union has developed its strategy on cybersecurity research in order to strengthen the confidence of European citizens in new technologies and insists on innovation that respects fundamental rights[3].

Besides that, we can note the existence of a European Research Area [24], which was created in 2000 to promote scientific and technological cooperation between Member States in order to establish a coherent European research policy. This makes it possible to create a common market for science, research and innovation, financed by the European Union. Its strategic support is the European Research Area Committee (ERAC)[4]. Another European research network has existed since

[1] https://www.larousse.fr/dictionnaires/francais/recherche/67011 ; https://dictionnaire.lerobert.com/definition/recherche ; https://www.larousse.fr/dictionnaires/francais/scientifique/71473 ; https://dictionnaire.lerobert.com/definition/scientifique.

[2] To this end, the Open Research Europe platform (https://open-research-europe.ec.europa.eu/) was launched in March 2021. As regards the pillars, we can mention firstly the strengthening of the EU's scientific and technological excellence and the European Research Area (science and technology). Secondly, responding to strategic priorities, including ecological and digital transitions and sustainable development objectives (society). And thirdly, boosting innovation capacity, competitiveness and employment (economy) [4].

[3] "Improving cybersecurity is therefore essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information" [25].

[4] https://www.consilium.europa.eu/fr/council-eu/preparatory-bodies/european-research-area-innovation-committee/

1971, the COST (European Cooperation in Science and Technology)[5], an intergovernmental structure for scientific cooperation. Other bodies exist to assist the development of European research, such as the European Innovation Council[6]; the ESFRI (European Strategy Forum on Research Infrastructures)[7]; or even the EIT (European Institute of innovation and technology)[8].

Finally, let us specify that articles 179 to 190 of the Treaty on the Functioning of the European Union provide the legal basis for actions in support of European cooperation in research and technological development.

2.1.2 The place of scientific research in the GDPR[9]

Personal data is defined as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly" (*Article 4.1, GDPR). We can expect that a massive amount of personal data will be collected to carry out research (identity of participants in a study and results, analysis of medical data, analysis of behaviour, etc.).

In contrast, we do not find a definition of scientific research in the GDPR. Only recital 159 of the GDPR gives some indication and called for a broad interpretation[10]. It includes notably technological development and demonstration. Additionally, the Article 29 Working Party (now replaced by the European Data Protection Board) considers that the notion of scientific research can more broadly cover any research project established that meets the methodological and ethical standards of the sector [8]. It should be noted that Recital 162 of the GDPR also gives some guidance on the concept of statistical research.

The GDPR allows for some adaptations to the specific situation of the use of personal data for scientific research purposes (see the section below for practical guidance on these derogations). These are the following principles:

- *Purpose limitation*. In principle, the controller of personal data must determine in advance and with precision the purpose he/she wishes to pursue (article 5 of the GDPR). By way of derogation, Recital 33 of the GDPR allows for some flexibility, with a constant and increasingly precise determination of the purpose as the research process evolves. This possibility offered by the GDPR cannot be interpreted as allowing the controller not to have to anticipate and specify the purposes of the research in advance [8, 9]. Any exception to a general rule must be interpretated in a strict way.

[5] https://www.cost.eu/
[6] Which supports the careers of researchers by offering grants: https://eic.ec.europa.eu/
[7] Which examines research infrastructure needs at European level: https://www.esfri.eu/
[8] Which seeks to increase Europe's competitiveness, sustainable economic growth and job creation by promoting and strengthening cooperation between key business, education and research organizations and by fostering innovation and entrepreneurship in Europe by creating environments in which creative and innovative ideas can flourish [5].
[9] For the legal framework concerning the scientific research in the GDPR, please see Recitals 19, 33, 50, 52, 53, 62, 65, 113, 156, 157, 159, 161, 162 and Articles 1.b, 5.1.e, 5.1.j, 14.5.b, 17.3.d, 21.6, 32, 89.
[10]"Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures", Recital 159 of the GDPR.

- *Compatibility* of the purpose of the research with the purpose for which the data were originally collected. The collection of personal data may consist of initial or further processing. Initial processing means that personal data are collected for the first time by the controller to carry out scientific research from the outset. This processing must be based on one of the lawfulness grounds listed in Article 6 of the GDPR (see also the point below on consent from the data subject for research purposes). When a natural or legal person wishes to re-use personal data for a purpose other than the original processing, the GDPR requires him/her to carry out an examination of the compatibility of the new purpose he/she wishes to pursue with the original purpose (Article 6.4 GDPR). If scientific research is not the purpose for which the data were originally collected (further processing), the GDPR admits an accounting in principle (Recital 50 and Article 5.1 b). In this case, the transparency obligations contained in the article 13, paragraph 3 and article 14, paragraph 4 shall apply [8].
- *Consent***.** When consent is the most appropriate basis to guarantee the lawfulness of the scientific research, the data controller may collect the consent of the data subject for a broadly defined purpose and give the possibility to consent to subsequent steps as the research progresses (see below) [8].
- *Storage limitation***.** Personal data may be kept longer than necessary to fulfil the original purpose in case of further processing for scientific research purposes. The safeguards provided for in Article 89 of the GDPR must be put in place (article 5.1e) of the GDPR).
- *Rights of the data subjects***.** Article 89.2 of the GDPR allows for certain derogations to the rights of data subjects provided that the derogation is necessary to achieve the purpose of the research. These are the right of access (article 15 of the GDPR), the right of rectification (article 16 of the GDPR), the right to the restriction of the processing (article 18) and the right to object (article 21 of the GDPR). There is no possibility of derogation for the right to erasure (article 17) and the right to data portability (article 20) in case of consent by the data subject to collect personal data for research purposes. This possibility of limiting the rights of data subjects might be under some guarantees put in place by the data controller by the law of each Member States. Additionally, article 14 of the GDPR provides for exceptions to data subject rights. Thus, special rules should apply when processing personal data for scientific research purposes as we explain in the following guidelines. Figure 1 outlines the different steps that should be followed by the data controller.

However, it is important that the GDPR leaves room for Member States to legislate in the specific context of scientific research. It is therefore important to check compliance with the GDPR but also with the applicable national law (recital 156 of the GDPR).

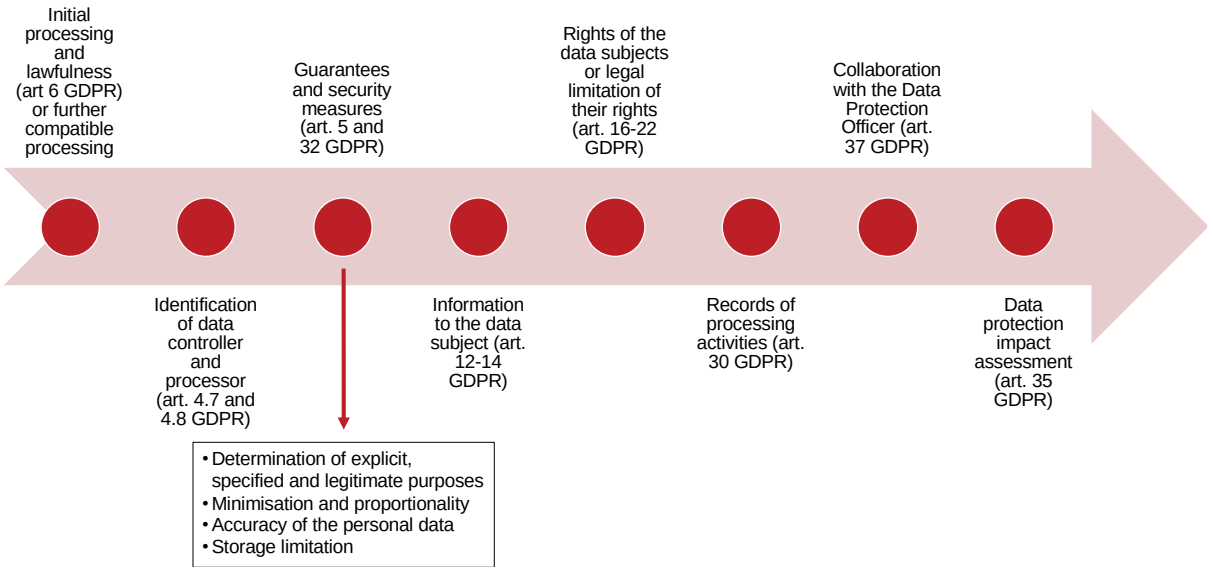


Figure 1: Timeline for compliance with the GDPR

2.2 Guidelines

2.2.1 Purpose and scientific research

In WP6, we have established the legal framework to preserve personal data in intelligent infrastructures and the privacy-enhancing mechanisms that could be used [38]. For the specific topic on AI, we refer to the deliverables D7.1, D7.2, D7.4 and D7.5 to develop the GDPR consideration (see also the work of the High-level Expert Group on AI [30, 31]).

As the GDPR mentions the importance and interest for society of processing operations carried out for scientific or historical research purposes as long as these processing operations comply with the personal data protection requirements of the Regulation (Recital 156 and 157, GDPR), the following guidelines are transversal to all the Programs.

Indeed, article 5(1)(b) of the GDPR provides that personal data may only be collected for "specified, explicit and legitimate purposes" which must in principle be defined prior to processing. However, Recital 33 acknowledges that it is not always possible to determine in advance the exact purpose of a processing operation carried out for scientific research purposes[11].

Note that the mere indication of "for research purposes" is not sufficient. A lack of precision regarding the purpose can be compensated by the controllers providing regular information on the evolution of the purpose as the project progresses so that over time the consent is as specific as possible. In this way, the data subject will have at least a general understanding of the state of play, which will enable him to assess whether he wishes to make use of his right to withdraw consent in accordance with Article 7(3) [8].

The establishment of a comprehensive research plan that data subjects could consult before giving their consent could also help to compensate for the lack of precision of the purpose. This research plan should describe the research questions and the envisaged working methods as clearly as possible. It could also contribute to compliance with Article 7(1), as controllers must be able to prove that the information was accessible to data subjects at the time of consent in order to demonstrate the validity of the consent [8]. The information must be comprehensive.

[11]"it is often not possible to fully identify the purpose of personal data processing for scientific research purposes at the time of data collection. Therefore, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research", Recital 33, GDPR

EXAMPLE: At the time of data collection, a research centre knows that it will process certain categories of research but does not yet know precisely what processing will be carried out. The research centre, which is responsible for the processing, may seek the consent of the data subject only for certain areas of research or certain parts of research projects, insofar as the purpose of the research permits (Recital 33, GDPR).

2.2.2 Further purpose when research results or raw data are to be re-used

The GDPR prohibits further processing if the purpose is not compatible with the initial purpose. This prohibition is lifted if the data subject consent (Article 6.4, GDPR). In determining the compatibility of purposes, account must be taken, inter alia, of any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; the nature of the personal data, the possible consequences of the intended further processing for data subjects; the existence of appropriate safeguards, which may include encryption, minimisation, anonymisation or pseudonymisation (Article 6.4, GDPR).

Nevertheless, the re-use of data for scientific research purposes is presumed to be compatible with the initial purpose of processing if appropriate safeguards are respected, in particular those referred to in Article 5.1.b) and Article 89.1. GDPR and the guarantees put in place at national level where applicable. The GDPR also states that if these initial or further scientific research purposes of the processing can be achieved without identifying the data subjects, this should be done.

In practice, the controller of research data may encrypt, pseudonymise or anonymise the data (making it impossible to identify individuals) provided, of course, that the purposes can be achieved in this way. It should be noted, however, that insofar as the scientific research purpose of the processing (or further processing) can be achieved without identification of the data subjects, the controller must go beyond pseudonymisation and must ensure that the data subjects are no longer identifiable (Article 89.1, GDPR). These measures are part of the Privacy by Design principle, which implies protecting personal data from the very beginning. This means that researchers are now obliged to integrate this principle of personal data protection into the implementation of projects involving data processing (Article 25, GDPR).

Finally, if the controller uses a subcontractor in this further processing, a subcontracting agreement should be drawn up which sets out the roles and responsibilities of each party, in particular the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller (Article 28.3, GDPR).

EXAMPLE: The data subject was not initially informed of the pursuit of a scientific research purpose. It is only later that the controller decides to pursue such a purpose. In this case, the appropriate safeguards referred to in Article 89.1 GDPR shall apply, for example by pseudonymising the data.

2.2.3 Lawfulness

Any processing of personal data, including for research purposes, must find its basis for lawfulness in one of the six possibilities proposed by Article 6.1 GDPR. At first glance, we might think that consent (Article 6.1. a), GDPR) is the most adequate basis for lawfulness. However, the European Data Protection Board ("EDPB") has expressed a clear opinion for clinical trials [16] that consent is not the most appropriate basis for scientific research. Indeed, the EDPB considers that the condition of freedom of consent could be biased in certain cases, for example in the context of clear imbalances between the data subject and the controller. This could be the case in the context of scientific or medical research that targets elderly people, who have not had access to a certain level of education or who live in a certain disadvantaged environment. The person concerned must understand

that he is the subject of a scientific study (principle of transparency) in order to be able to give informed consent [16].

In the past, the Article 29 Working Party already stated that "*at the same time, the GDPR does not restrict the application of Article 6 to consent alone, with regard to processing data for research purposes. As long as appropriate safeguards are in place, such as the requirements under Article 89(1), and the processing is fair, lawful, transparent and accords with data minimisation standards and individual rights, other lawful bases such as Article 6(1)(e) or (f) may be available.69 This also applies to special categories of data pursuant to the derogation of Article 9(2)(j)" [8].*

Where the research purposes cannot be specified in their entirety, the controller should find other methods to ensure that the essence of the consent requirements are met as far as possible, for example by ensuring that data subjects can give consent for a research purpose expressed in more general terms, as well as for any specific stages of the research project known in advance. As the research project progresses, consent for subsequent stages of the project may be obtained before these stages begin [8].

Other issues arise in the case of consent as a basis for lawful processing, in particular the question of withdrawal of consent and the fate of the processing activities. The EDPB responds that in this case, the controller must cease all processing and delete the data if no other legal basis can justify it. In the area of research, an exception exists which states that the right to erasure does not apply if it is likely to make it impossible or seriously compromise the achievement of the research objectives (Article 17.3.d), GDPR).

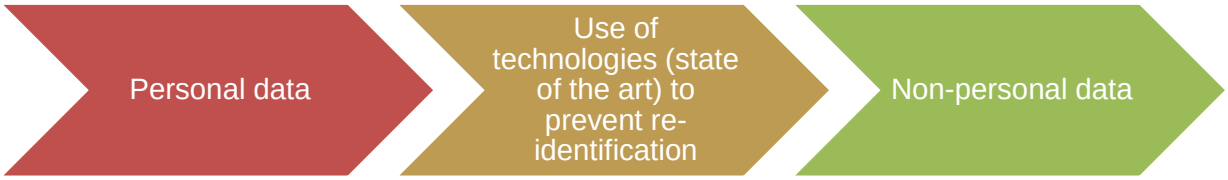
The EDPB therefore proposes that the public interest mission (Article 6.1.e), GDPR) or legitimate interest (Article 6.1.f), GDPR) should be the basis for lawfulness for research [16].

EXAMPLE 1: The processing of personal data in the context of clinical trials can thus be considered as necessary for the performance of a task carried out in the public interest when the conduct of clinical trials directly falls within the mandate, missions and tasks vested in a public or private body by national law [16].

EXAMPLE 2: For all other situations where the conduct of research cannot be considered as necessary for the performance of the public interest tasks vested in the controller by law, the processing of personal data could be "necessary for the purposes of the legitimate interests pursued by the controller or by a third party". In this case, it must be possible to justify that the legitimate interests pursued by the controller override the interests or fundamental rights and freedoms of the data subject (Article 6.1.f), GDPR).

2.2.4 Data minimisation

Data minimisation is a legal obligation under Article 5.1(c) of the GDPR which requires the controller to limit the processing of personal data to that which is necessary for the purpose previously determined. This principle of minimisation cannot be limited to the amount of personal data but requires the controller to define a global privacy policy which, by default, is the least intrusive of the data subjects' privacy. As an essential guarantee to ensure research that respects the right to privacy [8], the GDPR does not allow any derogation from this principle in the specific context of research and encourages the use of anonymised data and, where appropriate, pseudonymised personal data as a matter of priority (Article 89 GDPR). For example, it is important to consider not disclosing research results in an identifiable form if this is not relevant to the purpose of disclosure or decoupling identifying data from research data where the purpose of the research allows (Recommendation 09/2012, Belgian data protection authority). The following Figure 2 illustrates the differences between anonymised and pseudonymised data. The data minimisation principle requires to process in priority anonymised data or, if anonymised data is not appropriate for the purpose, to process pseudonymised personal data. Figure 3 mentions the steps to be followed to implement the data minimisation obligation.



- Anonymisation

- Pseudonymisation

Figure 2: Anonymised and pseudonymised data

See deliverable D2.3 for more information about the notion of anonymisation/pseudonymisation and how to evaluate an anonymisation solution.

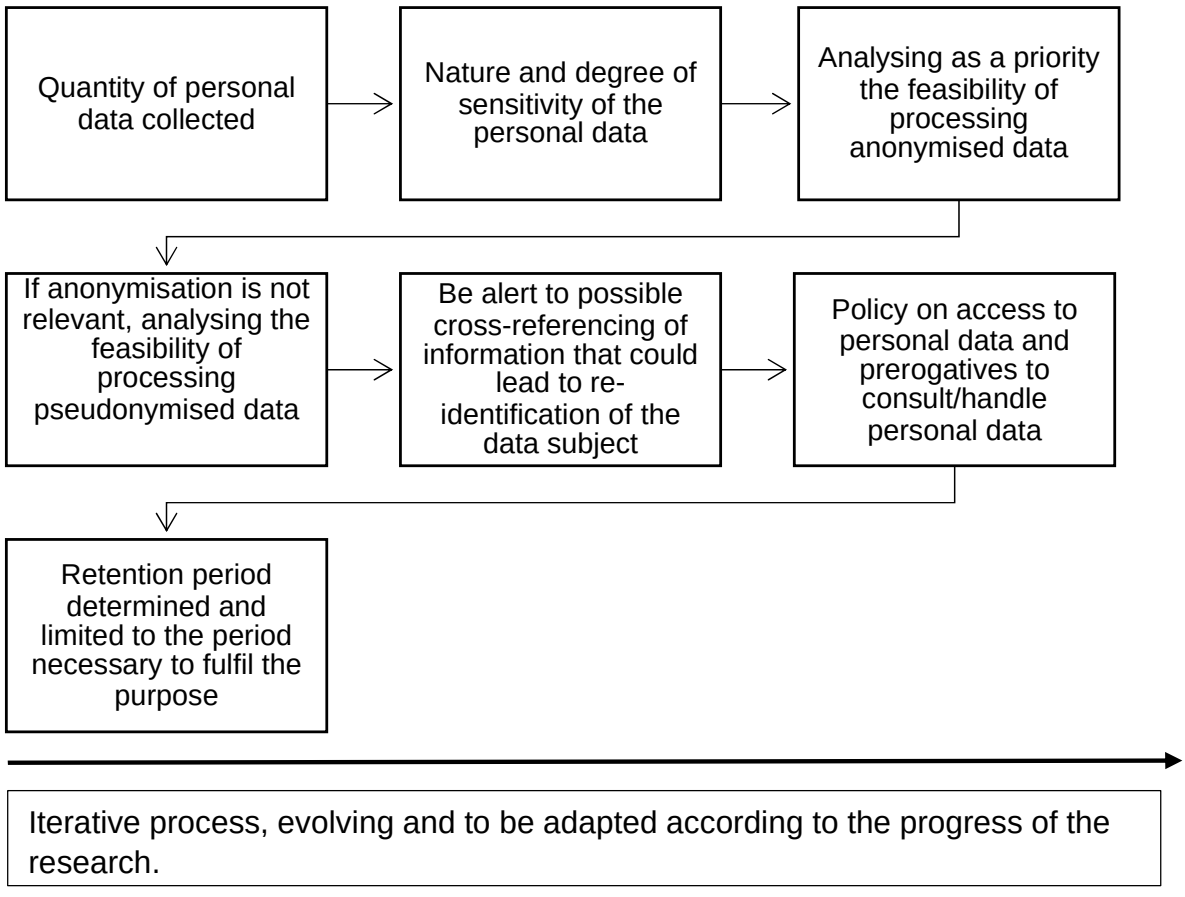


Figure 3: Data minimisation implementation

EXAMPLE 1: Article 201 of the Belgian law of 30 July 2018 on the protection of individuals with regard to the processing of personal data provides for when personal data are processed for scientific or historical research or statistical purposes by a data controller other than the original controller, the original data controller must anonymise or pseudonymise the data prior to their disclosure to the subsequent controller. The subsequent controller does not have access to the pseudonymisation keys.

EXAMPLE 2: Article 205 of the Belgian law of 30 July 2018 on the protection of individuals with regard to the processing of personal data prohibits the dissemination of non-pseudonymised data for research purposes, except with the consent of the data subject.

2.2.5 Sensitive data

The processing of certain categories of data is prohibited by the GDPR (Article 9.1, GDPR) [60]. In fact, by its nature, sensitive data is information that may have a particularly critical impact on an individual's privacy if it were revealed (Art 9.2.a), GDPR)[12]. It should be remembered that this requires increased vigilance when using them.

However, the text provides various exceptions, including one concerning research in Article 9.2.j). To benefit from this exception, several conditions must be satisfied. Firstly, the processing for scientific or historical research purposes must comply with the content of Article 89.1 GDPR based on Union law or the law of a Member State. Secondly, the processing must be proportionate to the purpose. Thirdly, it must respect the essence of the right to data protection and provide for appropriate and specific measures to safeguard the fundamental rights and interests of the data subject (Article 89.1 GDPR). In particular regarding the processing of genetic, biometric or health data, the GDPR allows Member States to maintain or introduce additional conditions, including limitations (Article 9.4, GDPR).

Moreover, Recital 53 of the GDPR specifies that special categories of personal data that merit higher protection should only be processed for health-related purposes if this is necessary to achieve those purposes in the interests of individuals and society as a whole.

EXAMPLE 1: An example is the processing of health data in the context of a pandemic, for scientific or historical research purposes, through studies conducted in the public interest in the field of public health. This processing may be carried out for quality control purposes or for information on the management and general national and local supervision of the health care system (Recital 53, GDPR).

EXAMPLE 2: The Belgian law of 30 July 2018 on the protection of individuals with regard to the processing of personal data in Article 9 specifies three additional measures to be taken when processing genetic, biometric or health-related data:

1° the categories of persons having access to personal data are designated by the controller or, where applicable, by the processor, with a precise description of their function in relation to the processing of the data concerned;

2° the list of the categories of persons thus designated is kept at the disposal of the competent supervisory authority by the controller or, where applicable, by the processor;

3° it shall ensure that the designated persons are bound by a legal or statutory obligation, or by an equivalent contractual provision, to respect the confidentiality of the data concerned.

[12]Sensitive data could be 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.

2.2.6 Transparency

The GDPR does not give a precise definition of the principle of transparency, but it can be understood as requiring that any information and communication relating to the processing of personal data should be easily accessible, easy to understand (use of a user-centric approach) and ensure clear and understandable language (Recital 39, GDPR). These transparency rules apply to the information to be provided to data subjects on the processing of their data (even if the personal data are not collected directly from the data subject) (Articles 13 and 14, GDPR), to the communication of data subjects' rights (Articles 15 to 22, GDPR) and in case of a data breach (Article 34, GDPR). At any stage of the research, the researcher responsible for the data processing must be transparent to the data subject, for example by clearly explaining the purpose of the research and the impact of the participation of the people concerned in the research. Where it is not possible for the researcher to provide the above information directly to the data subject or where this would require disproportionate efforts (e.g., in case of further processing), the researcher shall endeavour to disseminate this information in another way (Article 14.5.b), GDPR) [15].

Researchers responsible for processing data in research have an obligation that information and communications are concise, transparent, intelligible, and easily accessible, that they use clear and simple language, that they are provided in writing or by other means, including, where appropriate, electronically, or orally at the request of the data subject (Article 12.1, GDPR), and that they are free of charge (Article 12.5, GDPR). The guidelines on transparency under Regulation 2016/679 drafted by the Article 29 Working Party elaborate on these criteria and can help controllers better understand their obligations [9].

However, certain exceptions exist (Articles 13.4 and 14.5, GDPR), for example if the data subject already had the information (Articles 13.4 and 14.5, a), GDPR) or if the provision of such information proves impossible or would require disproportionate efforts, in the case of processing of data for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes. In such cases, the controller must take appropriate measures to protect the rights and freedoms and legitimate interests of the data subject (Article 14.5, b), GDPR). In this respect and as mentioned in recital 62, the number of data subjects, the age of the data, as well as any appropriate safeguards adopted should be considered (Recital 62, GDPR).

Finally, in case of transfers of data processed for scientific or historical research or statistical purposes, the legitimate expectations of society for the advancement of knowledge should be considered. As regards the principle of transparency in this respect, the controller should inform the supervisory authority and the data subject of the transfer (Recital 113, GDPR).

EXAMPLE: During a clinical trial, controllers must inform data subjects why they are participating in the trial, what data will be used, why they will be processed, etc. All this information must be easily understandable by the data subject. All this information should be easily understandable by the person concerned by the clinical trial. If this information is already known to the clinical trial applicant or if giving this information requires a disproportionate effort, then the data controller should put in place appropriate measures to protect the rights and freedoms and legitimate interests of the data subject.

2.2.7 Security

Appropriate security is an essential condition for the processing of personal data and provides an additional guarantee for the research activity [8]. Article 32 of the GDPR requires the controller to ensure the information and physical security of personal data. The security principle is not absolute and is determined according to:

- the state of knowledge and the costs of implementing security measures;
- the nature, scope and purpose pursued by the controller;
- the risks identified for the data subjects.

It is therefore security adapted to the seriousness of the risks incurred that is required by the regulations on the protection of personal data. This approach is called “the risk-based approach”. It will

help the data controller and the data processor to determine the technical and organisational measures that need to be implemented in order to minimise the identified risks. This approach promotes "a scalable and proportionate approach to compliance"[13] for security. Figure 4 illustrates the principle of the risk-based approach under the GDPR.

Figure 4: GDPR and risk-based approach

The Article 29 Working Party highlights that "*the scalability of legal obligations based on risk addresses compliance mechanisms. This means that a data controller whose processing is relatively low risk may not to do as much to comply with its legal obligations as a data controller whose processing is high-risk*" [10]. It adds that "*There can be different levels of accountability obligations depending on the risk posed by the processing in question. However, controllers should always be accountable for compliance with data protection obligations including demonstrating compliance regarding any data processing whatever the nature, scope, context, purposes of the processing and the risks for data subjects are*" [10].

ENISA adopted guidelines and a methodology to determine the probability of a risk could occur [18].

The aim is to prevent a personal data breach as far as possible, i.e., 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 (Article 4.12, GDPR). Figure 5 illustrates the different steps for a security policy.

EXAMPLE: Security measures must be strengthened when personal data, for the purposes of the research, cannot be pseudonymised. In case of pseudonymisation, the directory linking the pseudonymised data to information that clearly identifies the data subject must be protected by enhanced security measures.

[13] "Data subjects should have the same level of protection, regardless of the size of the organisation or the amount if data it processes. Therefore the Working Party feels that all controllers must act in compliance with the law, though this can be done on in a scalable manner" [10].

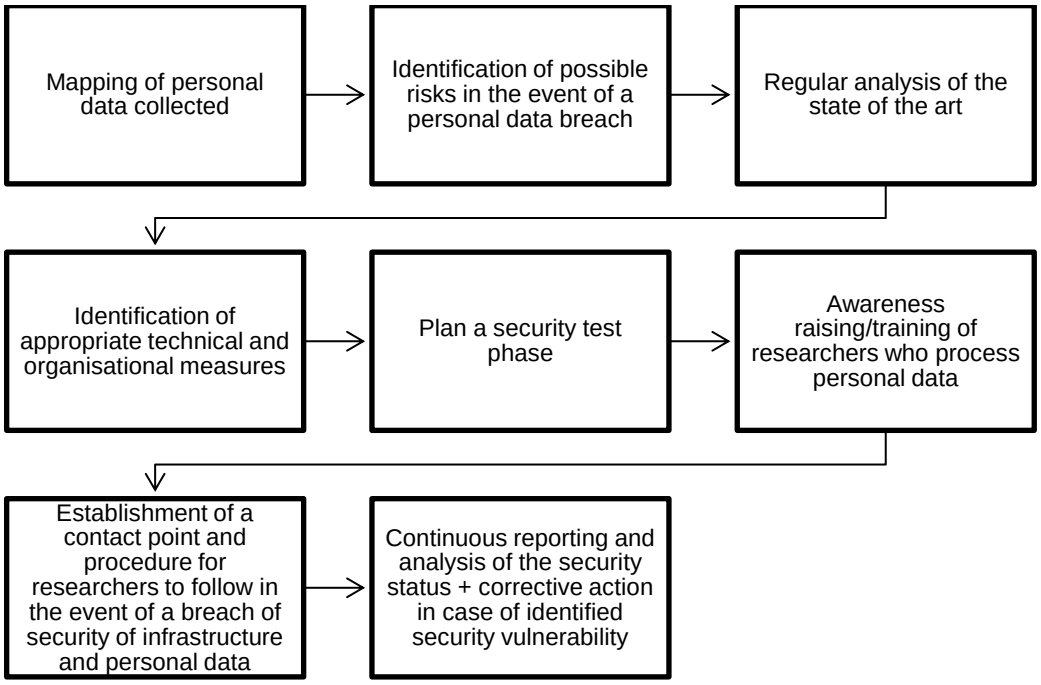


Figure 5: Security policy

2.2.8 Rights of data subjects

Various rights, developed in Articles 14 to 22 of the GDPR, are guaranteed to the data subject in relation to the processing of his or her personal data: the right to be informed, the right of access, the right of rectification, the right to erasure, the right to restriction of processing, the right to data portability, the right to object and the right related to automated decision-making including profiling (Articles 14 to 22, GDPR).

Article 89.2 of the GDPR states that Member States may provide exemptions to certain rights of data subjects in case of scientific or historical research purposes: the right of access, rectification, restriction, and objection (Article 89.2, GDPR). These derogations allow, among other things, to support and accompany the free flow of data exchanges in the scientific research sector.

Furthermore, the GDPR authorises Member States to provide specifications and derogations regarding data subjects' rights, under specific conditions and appropriate safeguards[14].

The Regulation provides examples of what such conditions and safeguards may include, such as specific procedures allowing data subjects to exercise these rights if appropriate for the purposes of the specific processing, or technical and organisational measures to minimise the processing of personal data in accordance with the principles of proportionality and necessity (Recital 156, GDPR).

EXAMPLE 1: The French law n° 78-17 of 6 January 1978 relating to data processing, files, and freedoms (transposing the GDPR) states in its Article 78 that a decree in the Council of State, issued after a reasoned and published opinion of the Commission nationale de l'informatique et des libertés (CNIL - French Data Protection Authority), will determine under which conditions and subject to which safeguards the rights of data subjects (access, rectification, restriction and objection) may be waived in whole or in part, with regard to processing for scientific or historical research purposes, or for statistical purposes.

[14] Recital 156 of the GDPR specifies that "Member States should be authorized to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes".

EXAMPLE 2: Article 186 of the Belgian law of 30 July 2018 on the protection of individuals with regard to the processing of personal data provides that if the exercise of the data subject's rights (right of access, rectification, restriction and objection) would make it impossible or seriously hamper the carrying out of processing for archival purposes in the public interest, for scientific or historical research purposes or for statistical purposes and where derogations are necessary to achieve these purposes, these derogations shall apply under the conditions determined by this law.

2.3 Conclusion

The ambition in this chapter was to list some general guidelines in the context of responsible and legally compliant cybersecurity research and innovation. Indeed, D2.6 closes this work package by analysing the concept of European scientific research and the strategy developed by the European Union in this regard, as well as the impact of the GDPR on this subject, to propose some practical guidelines for cybersecurity researchers.

The GDPR allows for some adaptations to the specific situation of the use of personal data for scientific research purposes. Thus, we have analysed the principles that particularly impact scientific research when processing personal data, such as purpose, lawfulness, data minimisation, sensitive data, transparency, security, and rights of data subjects. It should be borne in mind that the application of the provisions on the protection of personal data involves both technical and organisational dynamics at all stages of the research project: at the time of collection of the information, during its processing, and when the purposes of the scientific research have been achieved.

Finally, it may be interesting to note that other legislative instruments deal with data sharing, notably for research purposes. The European Union has adopted the Directive (EU) 2019/1024 on open data and the re-use of public sector information [3]. Any research data (defined as “any document in a digital form, other than scientific publications, which are collected or produced during scientific research activities and are used as evidence in the research process or are commonly accepted in the research community as necessary to validate research findings and result (Article 2.9 of the Directive 2019/1024[15]) should be made available for re-use by third parties. The Directive states that it should include research under public funding or co-funded by public and private-sector entities (Recital 28, Directive 2019/1024). Research data must be open, free of charge and in line with the FAIR principles[16].

We can also draw attention to a recent regulation from the European Commission: The Data Governance Act [6]. The third part of this legal instrument sets up a framework for altruistic sharing of personal data, notably to improve research within the Union. The aim is to strengthen the sharing of personal and non-personal data without reward for public interest purposes. The proposed Regulation does not define the notion of general interest. However, it specifies that the objectives are the fight against climate change, the improvement of mobility, official statistics, support for scientific research, basic research, applied research and privately funded research (Recital 35). The data shared by the altruism entity must be done with the consent of the data subject (in case of personal data) or with the authorization of the entity that collected in the first place the data (in case of non-personal data). To be considered as altruism, the legal entity of general interest must operate on a not-for-profit basis and must be independent from any entity that operates on a for-profit basis. The legal entity must respect several transparency obligations (Articles 15 to 22 GD).

Last but not least, a recent Commission proposal has been published: the proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of

[15]Recital 27 explains that “Research data includes statistics, results of experiments, measurements, observations resulting from fieldwork, survey results, interview recordings and images. It also includes meta-data, specifications, and other digital objects. Research data is different from scientific articles reporting and commenting on findings resulting from their scientific research”.
[16] See the regime provided for by article 10 of the Directive 2019/1024.

data (“Data Act”) [23]. This legal text lays down harmonised rules on making data generated using a product or related service available to the user of that product or service, on the making data available by data holders to data recipients (Article 1.1 and Chapters II and III of the Data Act). Chapter IV provides for rules to fight against unfair terms related to data access and use between enterprises. We should note the Chapter V which establishes a legal framework for mandatory data sharing (with certain limitations) from the private to the public sector in case of “exceptional need” (see Article 15 for situations falling under this criteria of exceptional need). Interestingly, Article 21 specifies that a public sector body or a Union institution, agency or body shall be entitled to share data received based on an exceptional need with individuals or organisations in view of carrying out scientific research (see also Recital 68).

Chapter 3 Encouraging Coordinated Vulnerability Disclosure: researchers' protection

3.1 Introduction

Sustainable development of infrastructure, as sought by the UN in the agenda for sustainable development [58], requires resilient IT solutions. However, any software may contain bugs or security holes, which can be exploited and cause harm. According to the Eurobarometer data, 28% of European SMEs have experienced at least one type of cybercrime in 2021 [34]. Businesses are mostly concerned with hacking online bank accounts and phishing, account takeover, or impersonation attacks, as well as viruses and spyware or malware [34]. The frequency of DDoS and ransomware attacks increased in 2020, the latter by 150% [19]. The ransomware attacks caused 18 days of downtime for an organization on average and the amounts to pay were doubled [28]. The threat to leak the data that was exfiltrated by the hackers increased from 8.7% in 2020 to 81% in 2021 [19]. Recent actions by Russia have shown that cyber-attacks are also used as a measure of hybrid warfare against private and public institutions seeking harm and paralysis of their functions. In June 2022, dozens of Lithuanian institutions, such as the State Tax Inspectorate and Lithuanian Railways, were attacked affecting their ability to perform their functions [42].

Prevention of cyber vulnerabilities is thus a problem that requires immediate attention and concrete solutions. Since the exploitation of network and information system vulnerabilities can lead to serious damage and disruption, the rapid identification and remediation of these vulnerabilities is a crucial factor in reducing cybersecurity risks [14]. Framework for early disclosure of vulnerabilities, particularly before the damage is done, is one of those solutions currently under development in the EU.

Coordinated (Controlled) Vulnerability Disclosure (CVD) is a process that allows IT vendors and finders of vulnerabilities to cooperatively discover solutions to reduce the risk associated with public vulnerabilities [35]. For instance, a researcher (finder) who discovered a flaw in a system, informs the developer (vendors, providers) of a system about a flaw and potential fixes. This allows the developer to take mitigation measures (patches, traffic monitoring, blocking) to eliminate or reduce the risk that the vulnerability is used by an attacker. Only then the vulnerability is published [50]. A researcher who discovers a system flaw informs the system developers of the deficiency and possible corrective actions. This permits the developers to take corrective actions to reduce the risk or neutralize the possibility of an attacker using the vulnerability. Only then the release of the vulnerability will be possible [35].

Given the gravity of the problem, the first policies and regulations were introduced over the last decade. Member States have approached the question under scrutiny in a different manner. Some countries (such as France or Poland) assure by the legal provisions that researchers will not face criminal liability, others do not provide a clear legal ground for such an assurance (for instance, Germany or Denmark). Other countries fear that the inclusion of CVD in national laws may enable hackers to access government systems without being held accountable [51]. On the other hand, the lack of clear policy and legal provisions making sure that researchers will not be criminally liable creates an obstacle for researchers to follow CVD procedures [51].

A lack of regulation in some states determines that voluntary schemes are brought to life by private companies. Since hackers frequently discover such flaws and, without the vendor's consent, disclose step-by-step instructions about vulnerability to the public, disregarding the possible IT security risk, vendors introduce responsible disclosure policies or "bug bounty" programs for the so-called "white hat" (and "grey hat") hackers [36].

The latter falls under the umbrella term of hacking performed in search of vulnerabilities (such as bugs, or gaps) in the IT system, to alert the owner of any risks they are not aware of [54]. These

activities are exercised for good – to help address security vulnerabilities and increase the security of IT systems [54]. The "white hat" hacking, i.e. hacking with the system owner's permission to test the resilience of a system usually raises no critical legal issues [54]. In contrast, "grey hat" hacking without malicious intent creates more legal ambiguity [54]. Legal vacuum and technicalities may subject such individuals to uncertainty – breaching an IT system without the owner's prior approval may, depending on the system and jurisdiction, amount to administrative or even criminal liability [54].

This situation leaves hackers in a predicament. On the one hand, they are encouraged by the company to disclose any exploits in exchange for a reward. On the other hand, they risk being prosecuted on the grounds of the formal composition of the crime. The owner of the IT system suffers too – even if the exploit of a system was found and reported, such action may formally amount to a data security breach subject to notification, resulting in additional administrative hurdles and even further formalities [54].

Various computer-related crimes are punishable under the national criminal law of different countries. The approach towards these crimes in the EU was harmonized by the Cybercrime Directive [1]. Several other regulatory initiatives were taken to fight the crimes and prevent them, where CVD was recognized as one of the effective means for improving the security of information systems [2]. Despite these efforts, cybersecurity experts doubt if the CVD mechanism may be effective at the EU level without harmonization efforts [17, 61]. Therefore, it is important to understand not only the possible need and added value of the EU-wide regulation, but also to identify which EU document would be the most suitable for this purpose.

Given the issues mentioned above, the main goal of the research of this section is to establish the differences in the scope of legal protection provided for vulnerability researchers at the national level, particularly considering possible negative consequences once the vulnerability is established and revealed. It discusses legal provisions regulating the process of CVD and criminal law provisions ensuring that vulnerability researchers will not face criminal liability. The analysis is limited to the overview of legislative perspectives of different EU countries since the existing regulation is compared with the aim to establish the scope of a common approach existing among the Member States. Furthermore, the section proceeds with the review of an existing regulation at the EU in this field and continues with the discussion on the possible need and added value of an EU-wide regulation obliging Member States to empower the CVD by establishing legal regulation protecting vulnerability researchers.

3.2 National approaches: from policy to legislative efforts

Based on the way countries approach vulnerability researchers' protection, in particular, issues related to criminal liability, countries can be grouped into several groups. The first group represents the Member States that have established a legislative framework guaranteeing the researcher who discloses vulnerability following strict conditions set by law will not face criminal liability. For instance, *France, Poland, and Lithuania* belong to this group of countries. Although the approach among the countries in this group differs, all of them ensure that if the researcher follows strictly established national procedure, s/he will not suffer any legal consequence.

For instance, in **France**, the law guarantees that a vulnerability discovery will not be prosecuted even if it usually constitutes a crime. Article L.2321-4 of the French Defence Code [55] ensures that the researcher or informant acting in "good faith" and transmitting the vulnerability to the ANSSI will not face criminal liability.[17] Article L.2321-4 of the Defence Code was reviewed in Article 47 of the Law for the Digital Republic, which established the CVD policy in 2016 [57].

Article 17 of the Cybersecurity Law of **Lithuania**, effective since 28 June 2021, guarantees that the search and disclosure of vulnerabilities will not result in criminal liability to the person who committed

[17] https://www.ssi.gouv.fr/en-cas-dincident/vous-souhaitez-declarer-une-faille-de-securite-ou-une-vulnerabilite/

such act only if the search for vulnerabilities is carried out in line of the restrictions set out in the law [40]. No respective changes were made along with the establishment of this regulation in the Criminal Code of Lithuania.

Although there is no consistent policy for managing CVD in **Poland** [17], in order to improve researchers' protection, security breaches in Poland were partially decriminalized in 2017 [17]. Articles 269b and 269c of the Penal Code of Poland establish the conditions where criminal liability does not arise under Articles 269b and 267(2) and 269a accordingly, i.e. if a person acts exclusively for the protection of an information system, an ICT system, or ICT network, or for developing a method for such protection (in case of both articles), and has immediately informed the holder of that system or network of the revealed threats, and his/her actions did not violate public or private interests or did not do any damage (additionally required by Article 269c) [49].

Latvia unsuccessfully intended to change its Law on the Security of Information Systems in 2016 to establish a legitimate background for the responsible vulnerability disclosure process by amending Section 241(3) of the Criminal Code of Latvia [36]. The amendment was supposed to guarantee that a person who submitted a responsible vulnerability disclosure report to the CERT about security flaws in systems, which process information related to the political, military, economic, social, and other security of the State and acted in compliance with responsible vulnerability disclosure policy will not be prosecuted [36].

Ireland does not have a policy in place since, according to the Irish government, the issue should be regulated at the EU level [17]. However, the legislation partially implementing the Cybercrime Directive leaves some room for vulnerability researchers' protection. Under the Criminal Justice (Offences Relating to Information Systems) Act 2017 [47], which took effect on 12 June 2017 and modernized Irish law on cybercrime, each of the offenses established in the Act requires to prove the absence of lawful permission, in addition, the offenses related to hacking and unsolicited penetration testing carry a further qualification *where a person or company had a reasonable excuse.* This term is not defined in the law and thus its interpretation is left to the case-law [44].

The other group represents the countries like *the Netherlands* and *Belgium*, that have CVD policies, however, the law does not provide any specific guarantee that the person disclosing vulnerability does not face criminal responsibility. The protection is applied in practice based on the concept that a criminal investigation is not instituted in case of legal rehabilitation between the discloser and the owner of the IT system.

The **Netherlands** is often presented as a CVD pioneer [36]. Although security researchers in the Netherlands were able to disclose vulnerabilities in a coordinated fashion already since 2008 [53], the first state-level responsible disclosure guidelines were published in 2013 by the National Cyber Security Centre [46]. It suggested that the organizations themselves could agree not to take legal action against the discloser following the disclosure guidelines [43]. However, if the Public Prosecution Service believes a crime has been committed, it may still bring charges [43].

The Dutch legislation does not include "ethical" hacking, nor does criminal law contain a provision ensuring that a discloser acting out of ideological or ethical motives will not face criminal charges. Addressing the problem, the Dutch Public Prosecution Service released a framework for handling coordinated vulnerability disclosure in March 2013 [51]. The Prosecution Service emphasizes the standard of the absolute necessity in the actions taken by a discloser to discover the vulnerability, thus the focus of the criminal investigation would be the evaluation if the actions were necessary and proportional under the given circumstances [51]. The new guidelines of 2018 did not change the rationale behind the Dutch CVD policy – if the researcher acts in line with the procedure established by the Dutch National Cyber Security Centre, s/he will not suffer legal consequences either. Avoiding negative legal consequences is possible only if an organization has a coordinated vulnerability disclosure policy [46].

Since 2018, the Belgium Public Prosecution office, the vulnerability reporter community, the commercial sector, and public agencies worked together with the Centre for Cyber Security **Belgium** on the creation of a national approach to CVD [17]. The Centre for Cyber Security Belgium published guidelines, which clarify the legal status of the researchers. In Belgium, a CVD policy or bug bounty

is based on agreements between the responsible organization and the researchers, outlining the contractual terms, typically published on a website [45]. Adopting such a policy denotes the responsible organization has given researchers permission to access or attempt to access the necessary IT systems to uncover any potential security flaws or to provide any pertinent information regarding their security. As long as the predetermined rules of the CVD are followed, access or attempts to access by researchers to certain IT systems is legal [45].

Germany and *Luxembourg* represent the countries where CVD policy is applicable only to the vulnerabilities of the software or hardware of the public sector. Researchers must follow the requirements established in the policy when disclosing a vulnerability. There are no specific legal provisions on avoiding criminal liability. On 21 October 2020, the Bundeswehr (the armed forces of the Federal Republic of **Germany**) published its Vulnerability Disclosure Policy [11], which is applicable only to the Bundeswehr's IT systems and web applications [12]. The Bundeswehr undertakes not to inform the law enforcement authorities of the findings if the security researcher follows the instructions of the Bundeswehr's CVD policy, unless criminal or intelligence intentions are pursued.[18]

Similar to Germany, the Responsible Disclosure Policy in **Luxembourg** addresses reporting of vulnerabilities occurring in software or hardware of the public sector [29], however, it does not address the private sector. Currently the platform GOVCERT.LU is used as a single point of contact to obtain and process vulnerabilities occurring in software or hardware of national institutions, agencies, or bodies that may have an impact on security [29]. There is no specific legislative framework enhancing the protection of cybersecurity researchers in Luxembourg, however, the Government considers it strategic to create a platform at GOVCERT.LU encouraging researchers to report vulnerabilities in the future [17, 26].

Finland has a CVD policy since 2010 [51]. CERT of Finland acts as a coordinator in the process of vulnerability disclosure, promoting the responsible handling of vulnerability information during all stages of the vulnerability life cycle [17].

In some countries there is no officially approved CVD policy, however, respective national authorities provide guidelines to facilitate vulnerability reporting. For instance, in 2019, the National Cyber Security Centre SK-CERT in **Slovakia** published a non-normative document "Vulnerability Reporting Guideline" [45]. The Guideline offers no guarantees for avoiding criminal liability if the procedure is followed, however, the SK-CERT emphasizes that certain activities must be necessarily avoided since they will be considered criminal offence [52].

In **Spain** there is no formal national CVD policy either, however, CVD policy was developed by INCIBE-CERT, the reference security incident response centre for citizens and private entities in Spain, which assists those who want to share information on vulnerabilities found both in INCIBE-owned CERT's systems and in the systems of other people or companies [32].

There are also countries that have neither a policy nor specific criminal law provisions, thus the vulnerability disclosure process is not standardized or regulated. However, vulnerability disclosure is in place through different policies of manufacturers. For instance, **Portugal** has no CVD policy, however, different software developers, hardware manufacturers, and service providers have established their own vulnerability disclosure policies (for instance Webcheck.pt platform[19]). Additionally, the proposal with a comprehensive CVD policy and legislative amendments, prepared by the task force, representing different stakeholders, including the amendments to criminal law is presented to the decision makers [17]. A National Cybersecurity Framework, developed by the Portuguese National Cybersecurity Centre in 2020 provides information on receiving, analysing, and responding to vulnerabilities disclosed internally or by external researchers [48]. While each organization is responsible for the development of internal CVD policy, the national CSIRT team will ensure the coordination of vulnerability response acting as a mediator [17, 48]. In **Sweden** there is no official CVD policy at the national level, the 2017 national cybersecurity strategy [27] does not include any intentions to

[18] https://www.bundeswehr.de/de/security-policy
[19] https://webcheck.pt/en/responsible-disclosure

develop it soon [17]. However, different manufacturers, like for instance Swedbank[20], use their own CVD policies or participate in private initiatives like HackerOne or OpenBugBounty to enable the reporting of vulnerabilities [17]. **Austria** does not have a CVD policy in place either, however, some private companies in the country handle vulnerability reporting according to established best practices. For instance, under the conditions of a bug bounty program of A1 Telekom Austria, everyone is eligible to participate in the program subject to its conditions[21]. Similarly, in **Italy**, where the CVD policy is currently drafted, many private companies use CVD policies for vulnerability disclosure [17]. In **Estonia**, it is commonly accepted in information security communities that the person who discovers a security vulnerability informs the owner of the system or service first [33]. The private sector and researchers are active in vulnerability disclosure; however, there is no formalized cooperation between these actors and respective governmental institutions [17].

To sum up, national approaches towards the level of coordination of vulnerability disclosure vary from country to country. Only four Member States have a comprehensive CVD policy, which includes different aspects of vulnerability researcher's protection. Five Member States enhanced the protection with the guarantee (at the legislative or practical level) that the researchers will not suffer negative consequences (in particular, criminal liability) if they comply with the strict requirements established in the national policy or with the CVD policies of different organizations. At least two Member States address the reporting of vulnerabilities occurring in software or hardware of the public sector and are planning to expand it to the private sector. In a number of Member States, where there is no standardized or regulated attitude towards vulnerability disclosure, the researchers are exposed to the variety of different policies of manufacturers. This does not stimulate vulnerability discovery and disclosure, but at least reduces the risk that the vulnerability researcher may face criminal responsibility. In the countries where these policies do not exist this risk is way higher, and the status of vulnerability researcher remains undetermined.

3.3 Different aspects of vulnerability researchers' protection

As observed by Ķinis [36], the generally recognized CVD lifecycle encompasses four phases: discovery; reporting; response; disclosure. All four phases are important for ensuring appropriate protection and recognition for security researchers. For instance, the stage of disclosure is usually associated with the acknowledgment of the security researcher and the right to get remuneration for the efforts. However, from the perspective of possible negative consequences, the stages of discovery and reporting are crucial. The discovery process is, firstly, related to the subjective side of crime. The reporting stage is associated with the strict procedure that has to be followed for the reporter to be exempted from criminal responsibility. The following subchapters discuss the conditions in which criminal responsibility do not arise and different guarantees in different stages of the vulnerability disclosure process.

3.3.1 Discovering vulnerability

3.3.1.1 Acting in "good faith"

Cybercrime Directive insists that in all cases, the criminal act must be committed intentionally [1], therefore it is logical that CVD policies require the reporters to have no malicious intents while discovering the vulnerability. Usually, there is no definition of good intentions in the policies themselves. A good intention often is presumed if the person who discovers and reports vulnerability, acts strictly following the established procedure and there is no abuse of vulnerability (see subpart 1.3.1.2.). However, some countries, like the Netherlands, provide an explanation of this element in the guidelines. It emphasized that the reporting party "wants to contribute to the security of IT systems by having this vulnerability remedied and possibly made public at a later stage" [46].

[20] https://www.swedbank.com/about-swedbank/contact-us/report-a-security-flaw.html
[21] https://www.openbugbounty.org/bugbounty/PaulMar23292621/

This element is particularly important in countries where there is a specific legal ground ensuring that a discloser acting out of ideological or ethical motives will not face criminal liability. For instance, Article 47 of the French Law for the Digital Republic creates a safe harbour for vulnerability reporters when one out of two criteria are strictly met, constituting a derogation to French criminal law "Researchers reporting a vulnerability must act in good faith, i.e., either knowing that they act within the boundaries of the legal framework, or that they reasonably ignore that they are acting outside of the legally authorized scope" [17]. Article 40 of the French Code of Criminal Procedure states that: "[...] Any constituted authority, public officer or civil servant who, in the exercise of his duties, acquires knowledge of a crime or misdemeanour is required to notify the public prosecutor without delay and to transmit to this magistrate all information, reports, and acts relating thereto" [56]. However, Article 47 of the French Law for the Digital Republic established that: "For the purposes of information systems security, the obligation provided for in Article 40 of the Code of Criminal Procedure shall not apply to a person acting in good faith who transmits to the national authority for the security of information systems information on the existence of a vulnerability concerning the security of an automated data processing system [...]" [57]. As we see legal definition of the term brings more clarity and legal certainty to the vulnerability reporters.

3.3.1.2 Abuse of the vulnerability

The list of prohibited actions that researchers may not ever perform is established by various above-mentioned cybersecurity agencies or governmental administrations as part of the CVD policies. Different EU member states have different approaches to the actions that researchers can or cannot take, however, some similarities may be observed.

Lithuania [39], Germany[22], Belgium[23], the Netherlands [46], Spain [32] prohibit researchers from copying, modifying, editing, or suppressing data from the IT system, modifying parameters of the IT system and attacking by a distributed denial of service (DDoS). Another common character in most of the countries is the prohibition of attacks through social engineering (Germany, Belgium, the Netherlands, Spain) and installing malware (virus, worm, trojan horse, or else) (Germany, Belgium, the Netherlands, Spain, Lithuania). Brute-force attacks to gain access to a system (in the Netherlands, Spain, Lithuania, and Belgium) and repeated access to the system or sharing access to the system with others (in Germany, and the Netherlands) are also mentioned by some countries as prohibited activities.

3.3.2 Reporting vulnerability

3.3.2.1 Subjects

The CVD policies in various countries use multiple terms to describe the subject who discovers and reports vulnerability. Some countries simply describe the subject by bringing in activities-related words. For instance, paragraph 2 of article 47 of the French Law for the Digital Republic mentions *the person who originated the transmission* [57], and Article 17 of Lithuanian Law on Cyber Security refers to a person who *discovered a vulnerability.* Other countries, institutions, or organizations use specific terminology. For instance, Belgium Centre for Cyber security utilizes the term a *CVD policy participant* and an *ethical hacker*. Slovakian National Cyber Security Centre refers to a *reporter (researcher, lab)*, the EU uses the term *vulnerability researcher* in the proposal for the reviewed NIS2 Directive, and ENISA mentions *security researchers involved in vulnerability discovery*. To compare, the U.S. Department of Health & Human Services also uses the term security researcher. However, as explained in the policy, the term *research* is described by a set of desired activities, as well as prohibited actions that would be regarded as illegal if proceeded.[24]

Usually, the CVD policies or specific legal acts do not provide the definitions of the above-mentioned terms, therefore, based on the general principle of law, these terms should be interpreted using the

[22] https://www.bundeswehr.de/de/security-policy
[23] https://ccb.belgium.be/en/faq-coordinated-vulnerability-disclosure-policy-cvdp-and-bug-bounty-programmes
[24] https://www.hhs.gov/vulnerability-disclosure-policy/index.html

ordinary meaning of the language of the legal act. There is no commonly accepted normative definition of a researcher, not to mention a security researcher. However, in some jurisdictions, the term *researcher* may have a normative definition in the legal acts, that are not directly related to cybersecurity. For instance, the Law on Higher Education and Research of Lithuania defines a researcher as "a person having a higher education" [41]. Therefore, Lithuanian Law on Cyber Security does not use the word *researcher* since it would limit coordinated vulnerability discovery to persons who have higher education in the sense that it would leave uncertainty as to the applicability of this procedure to those who are not highly educated. It is doubtful if the EU legislator or ENISA, summarizing the Members States' efforts in developing CVD policies and legislation had an intention to limit the circle of the subjects that can be engaged in vulnerability disclosure. In the view of the authors, this limitation would have no plausible explanation and would not definitely contribute to strengthening cybersecurity resilience.

3.3.2.2 Reporting procedure

Since there is no common approach to CVD, vulnerabilities' reporting procedures differ from country to country, where the process is coordinated by a national CERT, not to say from organization to organization where different organizations develop their own CVD policies.

For instance, some countries establish precise deadlines when a vulnerability must be reported. E.g., Lithuanian Law on Cyber Security obliges the person who has performed the vulnerability search no later than within 24 hours from the beginning of the vulnerability search (and if the search continues for more than 24 hours – every 24 hours), to prepare information about the results of the vulnerability search specified in the national vulnerability disclosure description (Article 17 of the law).

In countries, where the CVD policy is in place at a national level, national CERTs often, but not always, function as intermediaries. In some jurisdictions, coordinated vulnerability reporting must necessarily be conducted by contacting solely national CERT. For instance, one of the criteria mentioned in Article 47 of the French Law for the Digital Republic that vulnerability researchers must fulfil for avoiding criminal liability is that they report exclusively to ANSSI – no other public institution can receive a vulnerability notification. In other countries, regulations give the possibility to choose to submit the report directly to the organisation concerned or, alternatively, to a national CERT. Under the German Bundeswehr's vulnerability disclosure policy, whenever a vulnerability is discovered, reporters should use the contact form to get in touch with the Bundeswehr about the security problem and are asked to send the results by email. They must provide Bundeswehr with sufficient information so that they can reproduce and analyse the problem and provide a contact option for additional questions.[25] Lithuanian Law on Cyber Security obliges the person who has performed the vulnerability search to submit the report to the National Cyber Security Centre, or to the entity whose communication and information system has been searched for vulnerability [40]. The Dutch CERT may act as a mediator if the reporting of the vulnerability does not go as expected, or if a reporting party would prefer not to report the vulnerability directly to the organization. The National Cyber Security Centre attempts to put in contact with the reporter and the organization affected by a vulnerability after its reporting [46].

3.3.3 Anonymity v. visibility

3.3.3.1 Anonymity of the reporters

Protection of the identity of the vulnerability reporter is an essential guarantee. Although timely reporting of the vulnerabilities permits the relevant stakeholders, such as vendors and ICT infrastructure owners, to minimize the negative consequences on users, property, and reputation, this does not ensure that the manufacturer or operator of the vulnerable product or service would not undertake unauthorized recourse or intimidate the reporter [52]. For instance, Paragraph 2 of Article 47 of the French Law for the Digital Republic allows the person at the origin of the discovery of the vulnerability to remain anonymous, and the ANSSI preserves the elements of the declaration but also

[25] https://www.bundeswehr.de/de/security-policy

guarantees confidentiality of the identity [57]. Similarly to the French CVD procedure, the Bundeswehr offers the researcher to remain anonymous or, if he or she does not object, to communicate his or her identity to third parties. The German Bundeswehr's vulnerability disclosure policy ensures confidentiality of the report and will not pass the reporter's personal data on to third parties without his/her consent [17]. Likewise, in Slovakia, SK-CERT may contact entities concerned either with the reporter's identity or with the reporter's anonymity [52]. In Belgium, the confidentiality of the researcher and the exchange of information must also be ensured, however, it is important to mention that CVD in Belgium is based on the contractual provisions between an organisation and the reporter [17].

3.3.3.2 Acknowledgement

The need for an acknowledgment for a researcher having disclosed a vulnerability is approached differently due to the debate that it may also stimulate illegal hacking. For instance, the Bundeswehr ensures that reporters with successful submissions will be recognised on an acknowledgements page.[26] The Dutch National Cyber Security Centre suggests mentioning the name of the reporter if s/he wishes in a publication regarding the vulnerability [46]. The ANSSI on the contrary does not guarantee any acknowledgement for a reporter having disclosed a vulnerability to the agency.

3.3.4 Compensation

The question of whether to pay for the vulnerability reporters is disputable [53]. On the one hand, paying vulnerability disclosers can motivate people to share discovered flaws with the government and private organisations instead of using them offensively. Paying disclosers might be another method to appreciate the work and dedication of security researchers. On the other hand, there are concerns about the long-term effects, particularly regarding the labour rights of security researchers of the government potentially relying on an external, distributed workforce for vulnerability discovery and disclosure, as well as the ability of the government to pay remuneration due to administrative challenges related to the procurement policies and criteria [53].

Naturally, the countries address this question differently. Latvian CERT suggests that acknowledgment is a sufficient reward for reporting a vulnerability, therefore, no compensation is offered[27]. The Bundeswehr does not plan to offer bug bounties either.[28] On the contrary, the Dutch National Cyber Security Centre rewards every report of vulnerability depending on the quality of the report and the severity of the vulnerability [46]. Slovakian SK-CERT even encourages remuneration of the vulnerability reporters "to increase the security of the company's products and services". The reward may be offered by the company. In Belgium, a company can offer an award to the participant depending "on the amount, importance or quality of the information transmitted"[29]. ANSSI does not mention any compensation after a disclosure.

3.4 EU legislative approach

3.4.1 Current regulation

Ķinis [36] identifies the Proposal for a Council framework decision on attacks against information systems of 2002 [22] as the origin of the responsible vulnerability disclosure legal framework [36]. The adopted Council decision set a purpose to approximate criminal law around serious attacks against information systems by contributing to the fight against organized crime and terrorism, and therefore to ensure strong judicial cooperation in the area of criminal offenses related to attacks

[26] https://www.bundeswehr.de/de/security-policy
[27] https://cert.lv/en/about-us/responsible-disclosure-policy
[28] https://www.bundeswehr.de/de/security-policy
[29] https://ccb.belgium.be/en/faq-coordinated-vulnerability-disclosure-policy-cvdp-and-bug-bounty-programmes

against information systems [13]. Yet, it emphasized the "need to avoid over-criminalization, particularly of minor cases, as well as a need to avoid criminalizing right-holders and authorized persons" (Recital 13).

The Cybercrime Directive [1] amending and expanding the provisions of the above-mentioned Council decision, introduced a new regulation for harmonization of criminalization of a number of offenses directed against information systems and their penalties. Simultaneously, the Cybercrime Directive encouraged Member states "to provide possibilities for the legal detection and reporting of security gaps" (Recital 12). The EU legislator emphasized the effectiveness of identification and reporting of threats and risks posed by cyberattacks and the related vulnerability of information systems" to the "prevention of, and response to, cyberattacks and to improving the security of information systems" (Recital 12). The directive left a wide discretion to the national legislator in choosing how vulnerability disclosure is implemented in practice, while emphasizing that in absence of criminal intent or mandated testing or protection of information systems criminal liability should not be imposed (Recital 17).

In 2016, the NIS Directive [2] was adopted by the EU establishing minimum harmonization rules on vulnerability disclosure. The NIS Directive establishes that the announcement of incidents reported to the authorities should properly balance the public's interest to be informed about threats against the possible harm to essential services operators and digital service providers reporting incidents (Recital 59). Under NIS Directive, competent authorities and CSIRTs should focus on keeping strictly confidential information about product vulnerabilities before releasing adequate security fixes (Recital 59). At the same time, the NIS Directive was not intended to interfere with the Member States' right to safeguard their essential state functions, and to maintain law and order by pursuing an investigation of criminal offenses (Art. 1(6)). Yet, the issue of criminal liability for the illegal breach of information systems was already handled with the Cybercrime Directive. As the directive set only minimum rules on the matter, the Member States were left with a wide discretion that lead them to divergent practices concerning the criminalization of white hacking, as demonstrated above.

3.4.2 Current regulation

Cybersecurity experts doubt that the CVD mechanism may be effective at the EU level without harmonization efforts, therefore they suggest amending the Cybercrime Directive [17, 61]. For this purpose, they suggest amending the Cybercrime directive, namely directing the Member States to take the specific case of well-meaning hackers into account in their national legislation [61].

As demonstrated in the analysis above, a still relatively small number of EU Member States establish a legal basis assuring that criminal responsibility does not arise if CVD procedure is followed properly. This is usually done through certain provisions of criminal laws (e.g., Poland) or by introducing special provisions to the laws governing cybersecurity (e.g., Lithuania). Although the CVD policies in different countries provide the guarantee that researchers will not be prosecuted if they follow strict requirements established in the policy, in absence of a clear legal background in criminal law there is no certainty for vulnerability researchers that they will not be prosecuted for disclosing vulnerabilities in certain circumstances. Finding a vulnerability may involve breaking the law. In countries where vulnerability disclosure is left to the agreement between the organization and the researcher, like in the Netherlands, based on the CVD policy of the organization, the parties may agree that any possible criminal activities will not be reported [46]. However, this approach does not guarantee that a prosecutor will not start a criminal investigation *ex officio* believing that the policy boundaries were exceeded. Italian legal scholars and judges say that it would be shocking to leave it up to the judges to decide what constitutes unauthorized access to a system, as each judge is free to determine within its scope what should be considered ethical hacking and what should not be considered ethical hacking [17]. Moreover, this procedure is entirely dependent on the organizations' policy preconditions that the reporting party must comply with [46], which means that there is no common approach even at the national level since the vulnerability researchers must deal with a number of different CVD policies of various organizations.

Additionally, as observed in the Cybercrime Directive, the “transnational and borderless character of modern information systems means that attacks against such systems are often trans-border in nature” (Recital 27) [1]. In relation to this, the CEPS’s scholars accurately express doubt as to whether and how such policies like those allowed in the Netherlands would have a practical impact in the remaining jurisdictions where such policy documents would not be accepted in the judicial system of the remaining jurisdictions within the EU [51]. Another concern is whether the vulnerability researcher could avoid prosecution in the jurisdictions where the conditions for prosecuting illegal access are stricter [51].

Thus, it is obvious that an unambiguous provision in criminal law ensuring that vulnerability researchers will not face criminal liability, would not only ensure more legal certainty but would also bring more clarity to the legal environment in which vulnerability researchers operate by defining the conditions under which the identification and disclosure of vulnerabilities would not lead to a breach of criminal law.

It is obvious that existing legal regulation at the EU level encouraging the Members States to provide possibilities for the legal detection and reporting of security gaps in place for already a decade has not ensured a common approach towards the guarantees of security researchers. Since the EU law does not present an obligation to introduce the guarantee for not entailing liability in the criminal law, Member States choose different solutions, sometimes struggling with the desirable legislative changes at the national level (e.g., Latvian example to introduce changes to Latvian criminal law). Since the EU has already started the enhanced harmonization of legal regulation in this area, by introducing common definitions, incriminations, and sanctions, it would be reasonable to include a specific provision imposing the obligation on Member States to define the conditions under which the identification and disclosure of vulnerabilities will not result in incrimination. The remaining question is which EU legal act is the most suitable for this purpose, the NIS 2.0 or the Cybercrime Directive.

In the context of this discussion, it is important to observe that Italy proposed to amend the NIS 2.0 Directive by introducing the rule, not present in the initial proposal of the revised text of the legal act, that Member States are in charge of defining the conditions under which the identification and disclosure of vulnerabilities does not lead to a violation of criminal law [17]. The directive proposes that Member States designate a CSIRT in the role of ‘coordinator’ which would act where necessary as an intermediary between the reporting entities and the providers of ICT products or services [14]. The CSIRT coordinator should be authorized to identify, and contact concerned entities, support reporting entities, negotiate disclosure timelines, and manage vulnerabilities that affect multiple organizations (multi-party coordinated vulnerability disclosure) [14]. Additionally, it seems that under the finally agreed text of the revised NIS 2.0 Directive, the Member States are obliged to take measures to facilitate CVD by establishing a relevant national policy. Member States should address, as much as possible, the difficulties faced by vulnerability researchers, such as potential criminal liability under their national legal order.

From the perspective of the national law, it is not essential which EU legal act provides for the obligation to adopt a national law. From the perspective of EU law, the choice is determined by the EU's competence to regulate a specific area and thus also the field of the matter. Since the need for a common approach toward the exemption from criminal responsibility of security researchers relates to the harmonization of criminal law provisions, the revision of the Cybercrime Directive, as suggested by YesWeHack and ENISA, would be a more appropriate choice.

3.5 Conclusions and recommendations

Given the state-of-the-art of policies and legislation of the different Members States, it must be concluded that there is no uniform approach toward the protection of vulnerability researchers in the European Union mainly because only a few Member States have a comprehensive CVD policy, which includes different aspects of vulnerability researcher’s protection. Additionally, a couple of Member States address only the reporting of vulnerabilities occurring in software or hardware of the public sector, and several Member States that do not have a national CVD policy, provide CVD

guidelines. In some countries, there are still no national CVD policies, although the vulnerability disclosure process is widely practiced in the private sector with individual vulnerability policies in place.

Legal protection of a researcher may incorporate different aspects, first and foremost the rights and obligations related to vulnerability research, discovery, reporting, and recognition. The right to be acknowledged and the right to stay anonymous are two diagonally opposite interests of vulnerability reporters, that are ensured differently depending on the policy existing in the country. It is usually ensured in the countries where a national CERT acts as a mediator and may have limitations in those Member States where vulnerability reporting is based on contractual arrangements between an organization and the reporter. The right to be acknowledged and remunerated is recognized in some, but not all countries with a CVD, due to the differing considerations of the possible dangers of such stimulation. The obligation to act in good faith/have good intentions and follow strictly the procedure established in national or organization CVD policy is the requirement intrinsic for avoiding criminal responsibility. However, although there are similarities, the list of the prohibited activities while discovering vulnerability, or once it is discovered, differs even in the countries with a CVD policy on a national scale. Additionally, even though the national laws with the EU are harmonized in the cybercrime area based on the Cybercrime directive, the assessment of the subjective part of any possible crime will be impacted by diverging national case-law.

Only four Member States enhanced the protection with the guarantee (at the legislative or practical level) that the researchers will not suffer negative consequences (in particular, criminal liability) if they comply with the strict requirements established in the national policy or the CVD policies of different organizations. Avoiding criminal liability is approached mainly from two different perspectives: by establishing the “guarantee” clause in criminal law or another related legal act or, alternatively, by establishing the obligation to conclude the agreement on vulnerability disclosure with the manufacturer. In a number of Member States, where there is no standardized or regulated attitude towards vulnerability disclosure, the researchers are exposed to the variety of different policies of manufacturers. It does not stimulate vulnerability discovery and disclosure; however, it at least reduces the risk that the vulnerability researcher may incur criminal liability. In the countries where these policies do not exist, this risk is higher, and the status of vulnerability researcher remains undetermined.

It is obvious that existing legal regulation at the EU level encouraging the Members States to provide possibilities for the legal detection and reporting of security gaps in place for already a decade has not ensured a common approach towards the guarantees of security researchers. Since the EU has already started the enhanced harmonization of legal regulation in this area, by introducing common definitions, incriminations, and sanctions, it would be reasonable to include a specific provision imposing the obligation on the Member States to define the conditions under which the identification and disclosure of vulnerabilities will not result in incrimination. Since the need for a common approach toward the possible criminal liability of security researchers relates to the harmonization of criminal law provisions, the revision of the Cybercrime Directive would be a more appropriate choice.

Chapter 4 Summary and Conclusion

In this deliverable, two important legal fields for future cybersecurity research were discussed.

Firstly, we addressed how to deal with the large amount of often personal data in the field of research in a legally compliant manner. As with any scientific research involving personal data, a balance must be struck between the legitimate protection of data subjects' rights on the one hand, and the freedom of research and societal benefits of cybersecurity research on the other. Therefore, we have analysed the European scientific research and the strategy developed by the European Union and examined what impact the General Data Protection Regulation has in this regard. The aim was to formulate guidelines for researchers on how to strike a balance between privacy protection and the requirements of scientific research. Indeed, the General Data Protection Regulation allows for some adaptations to the specific situation of the use of personal data for scientific research purposes. However, it must be taken into account that the stricter general rules of data protection law must be complied with, for example, when data is collected not specifically for research purposes or when the research objective has been achieved - i.e., when the system goes into operation.

We also highlighted the implications of the provisions of Directive (EU) 2019/1024 on open data and the re-use of public sector information, which require that all data from publicly funded research should be made available for re-use by third parties free of charge and in accordance with the FAIR principles.

In the future, the provisions of the recently adopted Data Governance Act will be important, as it creates the possibility of altruistic data sharing to improve research for public interest purposes within the Union. Although the term public interest is not conclusively defined in the Data Governance Act, a socially pressing issue such as cybersecurity is likely to be included. Finally, the proposed Data Act foresees harmonized rules for fair access to and use of data. In particular the provisions for mandatory data sharing from the private to the public sector in case of “exceptional need” and the possibility to use this data for carrying out scientific research offers potential for cybersecurity research.

Secondly, we discussed the case of coordinated vulnerability disclosure (CVD), i.e., how to deal responsibly and legally with identified security vulnerabilities. Malicious actors around the world exploit vulnerabilities - weaknesses, susceptibilities or flaws in an asset, system, process or control that can be exploited by private and public sector agents and criminals for cyberattacks. As a countermeasure, a number of countries around the world have addressed this problem through the Coordinated Vulnerability Disclosure (CVD) policy. In some national jurisdictions, these measures include a legal framework for security research and vulnerability disclosure practices done in good faith. In the absence of such legal regulation, the detection and disclosure of vulnerabilities may lead to prosecution of the researcher under national criminal law. We have compared the legal and policy approaches to ensuring the protection of vulnerability researchers by discussing different safeguards at different stages of the vulnerability disclosure process. We found that there is currently no common approach to regulating CVD in Europe, the landscape is ranging from a complete lack of regulation to non-binding recommendations on how to deal with CVD, to a few countries that have already comprehensively regulated CVD. Countries with an existing CVD regulation have established procedures for what researchers must or must not do to avoid criminal liability. But even the lists of activities prohibited in vulnerability disclosure vary from country to country. This still makes it difficult for researchers who are detecting and eliminating cyber risks to work on a stable basis.

It is clear that this regulatory patchwork does not help to promote the politically desired identification and reporting of vulnerabilities. It would be desirable that, in the course of the current harmonisation of legislation in this area, common definitions, constituent elements and sanctions were also formulated to end the current legal uncertainty.

Chapter 5 List of Abbreviations

Abbreviation	Translation
AI	Artificial Intelligence
ANSSI	Agence Nationale de la Securité des Systèmes d'information
CERT	Computer emergency response team
CNIL	Commission nationale de l'informatique et des libertés
CSIRT	Computer security incident response team
CVD	Coordinated (controlled) vulnerability disclosure
DDoS	Distributed denial-of-service
EDPB	European Data Protection Board
EIT	European Institute of innovation and technology
ENISA	European Union Agency for Cybersecurity
ERAC	European Research Area Committee
ESFRI	European Strategy Forum on Research Infrastructures
EU	European Union
FAIR	findable, accessible, interoperable, re-usable
GDPR	General Data Protection Regulation
IT	Information technology
SMEs	Small and medium-sized enterprises
UN	United Nations

Chapter 6 Bibliography

1. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. Official Journal of the European Union L 218 (14.08.2013): p. 8-14.
2. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Official Joural of the European Union L 194 (19.7.2016): p. 1-30.
3. Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. Official Journal of the European Union L 172 (26.6.2019): p. 56-83.
4. Regulation (EU) 2021/695 of the European Parliament and of the Council of 28 April 2021 establishing Horizon Europe – the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination, and repealing Regulations (EU) No 1290/2013 and (EU) No 1291/2013. Official Journal of the European Union L 170 (12.5.2021): p. 1-68.
5. Regulation (EU) 2021/819 of the European Parliament and of the Council of 20 May 2021 on the European Institute of Innovation and Technology. Official Journal of the European Union L 189 (28.5.2021): p. 61-90.
6. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). Official Journal of the European Union L 152 (3.6.2022): p. 1-44.
7. Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 - the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC Official Journal of the European Union L 347 (20.12.2013): p. 104-173.
8. Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, 2017. 17/EN, WP 259. Brussels. https://ec.europa.eu/newsroom/article29/items/623051/en.
9. Article 29 Data Protection Working Party, Guidelines on Transparency under Regulation 2016/679, 2018. 17/EN, WP 260 rev. 01. Brussels. https://ec.europa.eu/newsroom/article29/items/622227.
10. Article 29 Data Protection Working Party, Statement on the role of a risk-based approach in data protection legal frameworks, 2014. 14/EN, WP 218. Brüssel. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.
11. Bannister, A., *German armed forces launch security vulnerability disclosure program*, in *The Daily Swig*. 18.05.2021. https://portswigger.net/daily-swig/german-armed-forces-launch-security-vulnerability-disclosure-program
12. Bundeswehr. *Vulnerability disclosure policy der Bundeswehr (VDPBw)*. 2021; Available from: https://www.bundeswehr.de/de/security-policy.
13. Council of the European Union, Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. Official Journal of the European Union L 69 (16.03.2005): p. 67-71.
14. Council of the European Union, Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive 2016/1148 - Presidency compromise proposal, 2021. 12019/4/21 REV 4. Brussels. https://data.consilium.europa.eu/doc/document/ST-12019-2021-REV-4/en/pdf.

15. de Terwangne, C. and K. Rosier, *Droit d'être informée de l'existence de traitements la concernant*, in *Le règlement général sur la protection des données (RGPD/GDPR)*, C. de Terwangne and K. Rosier, Editors. 2018, Larcier: Brussels.

16. EDPB, Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b), 2019. European Data Protection Board: Brussels. https://edpb.europa.eu/sites/default/files/files/file1/edpb_opinionctrq_a_final_en.pdf.

17. ENISA, Coordinated vulnerability disclosure policies in the EU, 2022. European Union Agency for Cybersecurity: Athens and Heraklion. https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu.

18. ENISA, Handbook on Security of Personal Data Processing, 2017. European Network and Information Security Agency: Heraklion, Greece. https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing.

19. ENISA, Threat Landscape 2021 (April 2020 to mid-July 2021), 2021. European Union Agency for Cybersecurity: Athens and Heraklion. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021.

20. European Commission. *European Innovation Scoreboard 2021*. 2021; Available from: https://ec.europa.eu/docsroom/documents/46013/attachments/1/translations/en/renditions/native.

21. European Commission, Horizon 2020 - The Framework Programme for Research and Innovation, 2011. COM(2011) 808 final. Brussels.

22. European Commission, Proposal for a Council Framework Decision on attacks against information systems. Official Journal of the European Communities C 203E (27.08.2002): p. 109-113.

23. European Commission, Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 2022. COM(2022) 68 final. Brussels.

24. European Commission, Towards a European research area, 2000. COM(2000) 6 final. Brussels.

25. European Commission and High Representative of the European Union for Foreign Affairs and Security Policy, The EU's Cybersecurity Strategy for the Digital Decade, 2020. JOIN(2020) 18 final. Brussels. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0.

26. GOVCERT.LU, Responsible Disclosure Policy (Version 1.0), 02.12.2019. CERT Gouvernemental Luxembourg: Luxembourg. https://www.govcert.lu/docs/POL226_Responsible_Disclosure_Policy_%28Public%29_1.0.pdf.

27. Government Offices of Sweden, A national cyber security strategy, 2017. Regeringens skrivelse 2016/17:213. Ministry of Justice: Stockholm. https://www.government.se/4ada5d/contentassets/d87287e088834d9e8c08f28d0b9dda5b/a-national-cyber-security-strategy-skr.-201617213.

28. Group-IB, Ransomware uncovered 2020-2021, 2021. https://explore.group-ib.com/ransomware-reports/ransomware_uncovered_2020.

29. High Commission for National Protection, National Cybersecurity Strategy IV, 2021. Le Gouvernement du Grand-Duche de Luxembourg: Luxembourg. https://hcpn.gouvernement.lu/en/publications/strategie-nationale-cybersecurite-4/strategie-nationale-cybersecurite-4.html.

30. High-level Expert Group on Artificial Intelligence, The Assessment List for Trustworthy AI (ALTAI) for self assessment, 2020. European Commission: Brussels.

31. High-level Expert Group on Artificial Intelligence, Ethics Guidelines for Trustworthy AI, 2019. European Commission: Brussels. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

32. INCIBE-CERT, *Vulnerability disclosure policy*. 2022. https://www.incibe-cert.es/en/what-is-incibe-cert/vulnerability-disclosure-policy

33. Information System Authority, Cyber Security in Estonia 2022, 2022. Talinn. https://www.ria.ee/sites/default/files/content-editors/kuberturve/kuberturvalisuse_aastaraamat_2022_eng.pdf.

34. Ipsos, SMEs and cybercrime, 2022. Flash Eurobarometer 496. European Commission: Brussels. https://europa.eu/eurobarometer/surveys/detail/2280.

35. ISO/IEC 29147:2018, Information technology - Security techniques - Vulnerability disclosure, 2018. International Stanardisation Organisation: Geneva. https://www.iso.org/standard/72311.html.

36. Ķinis, U., *From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach.* Computer Law & Security Review, 2018. **34**(3): p. 508–522.

37. Knockaert, M., et al., Ethical, legal and societal aspects, 2020. Deliverable 2.1. SPARTA Project (EU H2020, GA 830892). https://www.sparta.eu/assets/deliverables/SPARTA-D2.1-Ethical-legal-and-societal-aspects-PU-M12.pdf.

38. Knockaert, M., et al., *Privacy-by-Design in Intelligent Infrastructures*, in *Deep diving into data protection : 1979-2019 : celebrating 40 years of research on privacy and data protection at the CRIDS*, C. de Terwangne and K. Rosier, Editors. 2021, Larcier: Bruxelles. p. 309-343.

39. Lietuvos Respublikos Seimas, Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas (Law No XII-1428 of the Republic of Lithuania on Cyber Security), 23.12.2014. Vilnius. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee/asr.

40. Lietuvos Respublikos Seimas, *Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 pakeitimo įstatymas (Law No XII-1428 of the Republic of Lithuania on Cyber Security)*. 11.12.2021. https://www.e-tar.lt/portal/legalAct.html?documentId=67b9e0b07eb711e8ae2bfd1913d66d57

41. Lietuvos Respublikos Seimas, Lietuvos Respublikos mokslo ir studijų įstatymas (Law on Science and Studies of the Republic of Lithuania). Valstybės žinios 54-2140 (12.05.2009).

42. LRT (Lithuanian National Radio and Television), *Major incidents 'contained' after Lithuania gets hit with massive cyber attacks*. 28.06.2022. https://www.lrt.lt/en/news-in-english/19/1728365/major-incidents-contained-after-lithuania-gets-hit-with-massive-cyber-attacks

43. Martin, H., *Dutch disclosure guidelines*. 2013. https://www.virusbulletin.com/virusbulletin/2013/01/dutch-disclosure-guidelines

44. Morrissey, C. and K. Harnett, Cybersecurity Laws and Regulations Report 2022 Ireland, 03.11.2021. Global Legal Group: London. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/ireland.

45. NASK, Coordinated Vulnerability Disclosure (CVD). Summary of the session "Together-safer, stronger, smarter", 2021. NASK National Research Institute: Warsaw. https://cyberpolicy.nask.pl/wp-content/uploads/2022/04/EN_Coordinated-Vulnerability-Disclosure-CVD_-Summary-of-the-session-Together-safer-stronger-smarter.pdf.

46. National Cyber Security Centre, Coordinated Vulnerability Disclosure: the Guideline, 2019. The Hague. https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline.

47. Oireachtas Éireann, *Criminal Justice (Offences Relating to Information Systems) Act 2017*. 24.05.2017, Department of Justice: Dublin. https://www.justice.ie/en/JELR/Pages/Criminal_Justice_(Offences_Relating_to_Information_Systems)_Act_2017

48. Portuguese National Cybersecurity Centre, National Cybersecurity Framework Version 1.0 EN, 2020. Lisboa. https://www.cncs.gov.pt/docs/qnrcs-web-eng.pdf.

49. Radoniewicz, F., *Cybercrime and Cyberterorrism* in *Cybersecurity in Poland: Legal Aspects*, K. Chałubińska-Jentkiewicz, F. Radoniewicz, and T. Zieliński, Editors. 2021, Springer: Cham. p. 33–52.

50. Schmitz-Berndt, S. and S. Schiffner, *Don't tell them now (or at all) – responsible disclosure of security incidents under NIS Directive and GDPR.* International Review of Law, Computers and Technology, 2021. **35**(2): p. 101–115.

51. Schaake, M., et al., Software Vulnerability Disclosure in Europe: Technology, Policies and Legal Challenges, 2018. Report of a CEPS Task Force. Centre for European Policy Studies: Brussels. https://www.ceps.eu/wp-content/uploads/2018/06/CEPS%20TFRonSVD%20with%20cover_0.pdf.

52. SK-CERT, Vulnerability reporting guideline, 2019. National Cyber Security Centre, National Security Authority: Bratislava. https://www.sk-cert.sk/wp-content/uploads/2019/10/Vulnerability_reporting.pdf.

53. Stevens, Y., et al., See Something, Say Something: Coordinating the Disclosure of Security Vulnerabilities in Canada, 2021. Ryerson University: Toronto. https://www.cybersecurepolicy.ca/vulnerability-disclosure.

54. Teplõhh, D., et al., *Ethical hacking in the Baltics: Comparative legal map*. 11.02.2022, TGS Baltics. https://www.tgsbaltic.com/en/publications/ethical-hacking-in-the-baltics-comparative-legal-map/

55. The National Assembly and the Senate of France, *Code de la défense*. 2016: Paris. https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000033206854#:%7E:text=Version%20en%20vigueur%20depuis%20le%2009%20octobre%202016&text=L'autorit%C3%A9%20pr%C3%A9serve%20la%20confidentialit%C3%A9,celle%2Dci%20a%20%C3%A9t%C3%A9%20effectu%C3%A9e.

56. The National Assembly and the Senate of France, *Code de procédure pénale (Code of Criminal Procedure)*. 2022. https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071154/

57. The National Assembly and the Senate of France, *Loi n° 2016-1321 du 7 octobre 2016 pour une République numérique (Law No. 2016-1321 of October 7, 2016 for a Digital Republic)*. 2016: Paris. https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000033203174

58. United Nations, Transforming our World: The 2030 Agenda for Sustainable Development, 2015. A/RES/70/1. https://wedocs.unep.org/20.500.11822/9814.

59. Valutytė, R., et al., Key challenges and promising solution approaches, 2021. Deliverable 2.3. SPARTA Project (EU H2020, GA 830892).

60. Van Gyseghem, J.-M., *Les catégories particulières de données à caractère personnel*, in *Le règlement général sur la protection des données (RGPD/GDPR)*, C. de Terwangne and K. Rosier, Editors. 2018, Larcier: Brussels. p. 255-284.

61. yeswehack, *Coordinated Vulnerability Disclosure policy for a safer cyberspace*. 06.08.2020. https://blog.yeswehack.com/advocacy-policy/coordinated-vulnerability-disclosure-policy-for-a-safer-cyberspace/