applied sciences

MDPI

Article

Data Protection Heterogeneity in the European Union

Marko Hölbl *, Boštjan Kežmah and Marko Kompara

Faculty of Electrical Engineering and Computer Science, University of Maribor, 2000 Maribor, Slovenia; bostjan.kezmah@um.si (B.K.); marko.kompara@um.si (M.K.)

* Correspondence: marko.holbl@um.si; Tel.: +386-2-220-7361

Abstract: In light of digitalisation, we are witnessing an increased volume of collected data and data generation and exchange acceleration. Therefore, the European Union (EU) has introduced the General Data Protection Regulation (GDPR) as a new framework for data protection on the European level. However, GDPR allows the member states to change some parts of the regulation, and the member states can always build on top of the GDPR. An example is the collection of biometric data with electronic signatures. This paper aims to compare the legislation on data protection topics in the various EU member states. The findings show that the member states included in the study generally do not have many additional/specific laws (only in 29.4% of the cases). However, almost all have other/additional legislation to the GDPR on at least one topic. The most additional legislation is on the topics of video surveillance, biometry, genetic data and health data. We also introduce a dynamic map that allows for quick navigating between different information categories and comparisons of the EU member states at a glance.

Keywords: data privacy; GDPR; heterogeneity; European Union

Citation: Hölbl, M.; Kežmah, B.; Kompara, M. Data Protection Heterogeneity in the European Union. *Appl. Sci.* **2021**, *11*, 10912. https://doi.org/10.3390/app112210912

Academic Editors: Gianluca Lax and Federico Divina

Received: 14 October 2021
Accepted: 17 November 2021
Published: 18 November 2021

1. Introduction

Digitisation has increased the volume of data collected and, at the same time, accelerated the generation and flow of personal information. Practically every facet of life and the widespread use of the Internet in both private and business settings have greatly expanded data collecting and hastened the exchange of personal information. Therefore, the European Union has enacted the General Data Protection Regulation (GDPR) [1] as a new framework to substitute Data Protection Directive 95/46/EC. The GDPR is directly enforceable and applicable because it is a regulation rather than a directive, albeit it allows the individual EU member states to change specific provisions. In contrast to directives that bind the EU member states to the outcome they must achieve whilst leaving national authorities free to choose the form and method (in practice, supplementing existing legislation or adopting new legislation), the regulation is universally applicable and directly binding for all EU member states.

Because a large amount of personal data can be easily exploited and such data is starting to gain considerable value on the market, the EU authorities have decided on single legislations to strengthen individual's rights across the EU and ensure uniform and coordinated action across the member states following years of deliberation. This has been done to prevent exploitation of the collected data and ensure a protection requirement that all personal data processors have to meet to defend against malicious actors. The final goal of the EU is to create a unified European digital market, free of regulatory restrictions imposed by the individual member states. The GDPR regulation applies to data of EU citizens regardless of the businesses' location or location of the processed data.

However, as we have eluded to before, GDPR allows some of its sections to be defined differently by the member states to better suit their needs and wishes. The prime example of this is the consent age (GDPR, Article 8, paragraph 1) set at 16 in the GDPR (persons aged 16 years and older do not require parental consent). However, the regulation allows

individual countries to change this to any age between 13 and 16. Member states can also have additional legislation that builds on top of the GDPR.

In this paper, we have collected information from supervisory authorities (SA; a.k.a. Data Protection Authority—DPA) of EU member states to investigate the situation on additional legislation on data protection extending the GDPR. The aim of the research is to show the extent of heterogeneity in data protection in the EU. The member state supervisory authorities were selected as the best source of information on national legislation and policies, as they are responsible for supervising the data protection laws applicable in their country. This research enables an overview of data protection legislation on some topics in an individual member state and the possibility to compare differences between EU countries. Moreover, we created a dynamic map that visualises the aforementioned data protection legislation heterogeneity and allows an interactive and easy way of comparing legislation on specific topics between the EU member states at a glance.

In the remainder of this paper, we first address other related work that collected and studied similar information. We follow with a survey outline, where we discuss why we designed the survey in the way we did and why we chose to collect particular data. In the section on data collection, we focus on the process of collecting data and present the full list of the collected data topics. Then we move on to the presentation of the collected information, its analysis and the discussion. We conclude the paper in the final chapter.

2. Related Work

Cataloguing and/or comparing legislation between countries can be very difficult, especially when done on any larger scale. The subject itself is very complex and, at times, convoluted. When this is done internationally, the complexity of local languages (often national legislations are not translated or easily accessible) makes it almost impossible for a small group to achieve. Therefore, these types of research are usually done by large organisations which either have contacts in many countries or are reputable enough to get help in any country they need. The alternative approach we used is to survey people for each of the required locations to get them to give you the wanted information, which is not difficult to obtain for them.

For the specific field of data protection, there has not been much study of relevant legislation on a large scale (i.e., including many countries) or comparison between them. However, we have found three [2–4] such collections that include many countries. Two of the three studies are worldwide in scope and cover many countries, albeit with limited scope as they only link privacy legislation to each of the included countries. The third study remains at the same level of legislation identification but with fewer discussed countries from around the world. While in these studies, the GDPR is mentioned in the EU member states, it is not the focus of the studies and is not discussed in any detail. These studies, therefore, only contain a list of relevant legislation and not much information on what the laws themselves dictate. They are not targeting GDPR issues (and are not centred on the EU) and do not give the users anything to compare policies across multiple countries.

S. Park et al. [5] surveyed the state of data protection legislation in the selected countries in relation to the implementation of digital forensic readiness. The authors looked at, among others, the EU as a unit and at Germany as a specific representative. For the EU, the focus was the GDPR with additional legislation present in Germany and its effects. The French supervisory authority, CNIL, has prepared a solution for a very specific condition set by the GDPR (Article 45), under which the transfer of personal data to third countries is allowed if the European Commission has confirmed a suitable level of data protection provided by the receiving country's national laws. The CNIL's map [6] on data protection around the world illustrates which countries have adequate data protection laws and for which other means of sufficiently protecting the data must be guaranteed before transferring the data.

The possibility of adapting and modifying the GDPR by each of the member states with national law derogations was purposefully a part of the GDPR (e.g., Chapter III Section 5

and Chapter IX) to allow for greater flexibility. W. Long and F. Blythe [7], A. Clearwater and B. Philbrook [8], and J. Vangadesan and N. Pook [9] discuss the most probable areas for derogations in GDPR. A comparison of privacy and data protection legislation and policies in the EU (looking at eight member states, including the United Kingdom) was performed by B. Custers et al. [10]. The study also considered the importance/situation of data protection in a country by looking at the general public's awareness, media coverage, its importance in political debates, etc. However, the research was conducted shortly before the GDPR came into force. While the study did consider the upcoming regulation, it could not predict the changes in national legislation.

Finally, three studies are the closest to the work of this paper. All three are centred on identifying derogations from the GDPR and how it is supplemented in the EU. The first [11] covers 16 current member states. The second study [12] included 13 member states, while the third survey [13] collected information for 21 member states. All three were made before the UK's exit from the EU and, as a result, also include data for the UK. All three collections provide relevant information from national legislations and policies for a variety of topics. There are only two general topics present in all three that we have also included in our study—the processing of sensitive data and the designation of a data protection officer. Other topics that have some overlap with our study include information on communication with SAs, data protection for employees, consent for children, and processing of the deceased's data. All three studies present the results in a textual form. While this allows for more information, it is less than ideal for comparison (there is still a lot of work on the user to extract the necessary information and compare), especially as the level of detail is often different between countries. Our study collected more targeted information that allows for easier comparison between the member states.

3. Survey Outline

In the chapter on related work, we have mentioned some studies that have collected derogations permitted by the GDPR in the EU member states. When designing our own aspects to compare in the EU, we have decided to go a different route and focus on topics that could potentially also affect how data protection is implemented differently between the member states regardless of GDPR. One such example is the collection of biometric data on electronic signatures. Firstly, we want to distinguish electronic signatures, which we are talking about, and are typically obtained by signing your name on a type of touchscreen, from digital signatures, which are a cryptographic authentication mechanism and technically a specific subsection of electronic signatures [14]. When signing your name on an electronic device, sensors can measure the pressure of the pen, the speed, the tilt, etc., of the signing process. All of these data are considered biometric data because they are produced from the technical processing of a natural person's physical, physiological, or behavioural characteristics. Similar signature characteristics can be obtained from close examination of actual physical signatures, which is why just mimicking the look of a signature does not make a convincing forgery (at least to an expert). This is the same reason why the biometric data is collected during an electronic signature. However, some countries do not allow the processing of biometric data for this purpose, meaning electronic signatures are nothing more than images of signatures. Such differences between the member states have the potential to cause problems related to the legitimacy of signatures, where a signature could be valid in one country but invalid in another (either because it does not contain biometric data, or because it does and is consequently a case of illegal processing of biometric data).

Some important aspects of data protection that often involve personal information are not discussed much in the GDPR and could become troublesome to implement under its requirements. Here we are primarily thinking of the processing of personal data in audit trails and the problems surrounding the processing of personal data in backups. Therefore, we were interested if individual member states have made legislation to more clearly define the requirements and how they can be achieved. Note that the results are only limited to

legislation and do not include any guidelines or rulings that supervisory authorities might have made on how personal data should be handled in audit trails and backups.

The inclusion of anonymisation as a form of avoiding complying with the GDPR and pseudonymisation as a method of complying with the GDPR is very interesting, especially with the open questions of when personal data become truly anonymous and how can we tell. Therefore, we were interested in whether any member states have additional legislation on the two topics where they might explain the requirements in more detail. Finally, as already discussed in the related literature, we have also included some of the topics included in the previous studies.

Collecting the data for the member states on our own was not an option. The information from foreign legislation and policies would be far too time-consuming if at all possible because they might not have an English translation. That is why we chose to use a survey. The first time, we have distributed the survey among CyberSec4Europe [15] project partners (this work was made as part of the project). With more than 40 partners, the project covers the majority of the member states. The survey was given to data protection officers (DPO) of the partner organisations. By collecting multiple responses for the same country, we were able to check for the consistency of the replies. Unfortunately, the results were very inconsistent, and we received varied feedback for the same member state. While this was a problem, it did give us an interesting insight. Even though DPOs know national data protection laws and policies fairly well, they cannot provide consistent information, indicating that this is a very complex subject. At the same time, it is understandable that DPOs, who typically deal with issues related to organisations they work in, might not have the information to the very specific questions from the survey. Ultimately we decided to scrap the collected data, and a more ambitious plan to contact all the supervisory authorities and collect the data from them was made.

4. Data Collection

To collect the best possible data quality, we chose to collect the data directly from national supervisory authorities (SA). A SA is an independent public authority that supervises the application of European data protection law, including GDPR. Each EU member state has to have a SA, which has investigative and corrective powers, provides expert advice on data protection issues, and handles any raised complaints. However, collecting responses from SAs is more difficult because there is only one per member state, and they might not be inclined to participate in unsolicited research. Even though they are the best entity to answer the prepared data protection questions, we expected to not get a response from every SA. To have the best possible feedback, we have repeatedly asked for their participation and have collected the data between April 2020 and June 2021.

The information gathering was centred around processing different forms of (special) data (e.g., biometrics) and any additional legislation or policies upgrading the GDPR requirements. The survey collected data for the following topics:

1. Any other legislation on the use of biometry (other than the GDPR).
2. Any other specific legislation on privacy, specifically with relation to:
    a. Video surveillance,
    b. hotography,
    c. Anonymisation,
    d. Pseudonymization and/or,
    e. Audit trails.
3. Any additional legislation that extends specific sections of the GDPR, specifically with relation to:
    a. Verification of parental consent,
    b. Processing data of the deceased,
    c. Processing of genetic data,
    d. Use of biometric data for the purpose of identification,

e. Processing of health data,
f. Processing of data on the sex life of individuals,
g. Processing of data on sexual orientation,
h. Erasure of personal data,
i. Data protection officer designation/appointment, and/or,
j. Supervisory authority consultations.

4. Presence of additional legislation on backing up of data.
5. Whether or not the use of biometrics is allowed for the electronic acquisition of handwritten signatures.
6. Whether or not the use of biometrics is allowed in a work environment (e.g., opening of server rooms with a fingerprint).
7. Minimum age of persons that do not require consent from a holder of parental responsibility.

5. Analysis of the Results and Discussion

In the survey, we collected feedback from 19 (Austria, Belgium, Croatia, Cyprus, Czechia, Denmark, Estonia, Finland, Germany, Greece, Hungary, Latvia, Luxembourg, Malta, Poland, Romania, Slovakia, Slovenia, and Spain) out of the 27 EU member states. The responses were collected between April 2020 and June 2021 in many repeated solicitations of supervisory authorities to participate in the survey.

We compared the collected data with the complementary data from [12,13] previously mentioned in the related work section. The most similar data collected and, therefore, the most appropriate for comparison were the data regarding the age of consent for children and the additional regulations surrounding the data of the deceased. The consent age, which we could compare with both other studies, was identical in all three studies except for the information on the Czech Republic. The result from [13] indicates the consent age is 13, while our inquiry and that of the [12] received information that it is 15. We were able to confirm from a separate source that the consent age in the Czech Republic is, in fact, 15 years of age. The information on the additional legislation surrounding the processing of deceased person data was only collected in [12], and we could therefore only compare our results to theirs. The cross-section of the collected results in the two studies did not show any mismatch. The two points of comparison give us high confidence in the trustworthiness of the data collected in our study.

Table 1 represents the collected data from the supervisory authorities. In the table columns are the 19 member states that we have collected the data for. Rows represent the topics (i.e., questions in the survey) for which we have collected data. Rows or rather topics are marked with the same numbers and letters as previously listed in the survey outline section. For example, any specific legislation on video surveillance is marked with *2a* because in the previous section, "Any other specific legislation on privacy, specifically with relation to" is numbered with a *2* and "Video surveillance" is under point *a*.

The answers "yes" (the member state has additional or more specific legislation on the topic) and "no" (the member state does not have additional or more specific legislation and the original GDPR applies) that are represented by the cross-section between the member states and topics in Table 1, are colour-coded green and red, respectively.

Topics marked from 1 to 4 contain the information on whether or not a member state has additional/specific legislation on that topic. How many of the topics are covered with other or additional legislation (number of green squares for each of the member states) is summed in a row marked as "SUM". Topics marked with the numbers 5 and 6 are specific questions regarding the use of biometrics, and we do not include them in the analysis of specific or additional legislation in the member states. They are also different because the green colour of a cell in these two rows means that a member state allows the use of (not that it has additional legislation on like in previous rows) biometrics for the electronic acquisition of handwritten signatures (row marked with No. 6) or biometrics in a work environment (row marked with No. 7). The very last parameter (row marked with No. 7) is the consent age—the age after which individuals no longer need parental consent. We also

produce the total number of green cells across all member states included in the survey for each topic. This information is in the far most right column (marked "SUM"). It gives information on how commonly a certain topic is covered in additional legislation (topics marked 1–4) or how frequently the use of biometrics is allowed for collecting signatures or in a work environment (topics marked with No. 5 and 6) across the member states.

Table 1. GDPR heterogeneity in the EU.

	Austria	Belgium	Croatia	Cyprus	Czechia	Denmark	Estonia	Finland	Germany	Greece	Hungary	Latvia	Luxembourg	Malta	Poland	Romania	Slovakia	Slovenia	Spain	SUM
1																				11 (58%)
2a																				15 (79%)
2b																				1 (5%)
2c																				2 (11%)
2d																				3 (16%)
2e																				4 (21%)
3a																				4 (21%)
3b																				4 (21%)
3c																				12 (63%)
3d																				9 (47%)
3e																				11 (58%)
3f																				2 (11%)
3g																				2 (11%)
3h																				5 (26%)
3i																				4 (21%)
3j																				5 (26%)
4																				1 (5%)
SUM	3	5	6	4	1	4	3	13	8	2	10	8	0	0	1	6	6	3	12	
5																				10 (53%)
6																				15 (79%)
7	14	13	16	14	15	13	13	13	16	15	16	13	16	13	16	16	16	16	14	

Red cells are "No" answers to topics defined in Section 4. Green cells are "Yes" answers to topics defined in Section 4. For full details, please refer to Section 5.

The results show that in the majority of the cases, member states do not have many additional/specific legislations. We have found that only 95 cases have additional/specific legislation (topics marked from 1 to 4) of the maximum possible of 323—which is 29.4%. This can be seen from the predominately red colour of Table 1.

The topics most often additionally covered with legislation other than the GDPR are in the area of biometry use (row marked with No. 1; in 11 of the 19 countries), video surveillance (2a; 15) processing genetic data (3c; 12), using the biometric data for the purpose of identification (3d; 9), and processing of health data (3e; 11). On the other end of the spectrum is the legislation on photography (2b) and data backups (4) which have further legislation only in one member state each. They are closely followed by additional legislation on anonymisation (2c) and extensions on GDPR rules regarding the processing of data on the sex life (3f) and sexual orientation (3g), each with legislation in only two countries.

Luxemburg and Malta are the only countries that do not have any additional legislation on the topics covered in our survey; all others included member states have at least one topic where they have other/additional legislation to the GDPR. Other countries with little additional legislation on the topics covered in this survey (topics marked from 1 to 4 in Table 1, up to a maximum of 17) include Czechia (1), Poland (1), and Greece (2).

Based on the feedback from the SAs, the most additional legislation relevant to the discussed topics are in Finland (13 green fields in topics from 1 to 4, from possible 17), Spain (12), Hungary (10), Germany (8), and Latvia (8). The use of biometrics for the

electronic acquisition of handwritten signatures (row marked with No. 5) is allowed in 10 of the 19 surveyed countries—so a very even split. In contrast, only four member states do not allow biometrics in a work environment (row marked with No. 5; Greece, Malta, Slovakia, and Slovenia). This could indicate that the member states are interested in limiting the use of biometric data but do not wish to limit businesses.

The results of the survey have also been integrated into a dynamic map, enabling quick navigation through the different topics of information and comparison of the EU member states at a glance. The map has been published and can be found at [16]. The published map is depicted in Figure 1. The figure also shows what specific additional legislation is present in Spain, but naturally, users can hover over any of the countries covered in the survey to get its information.

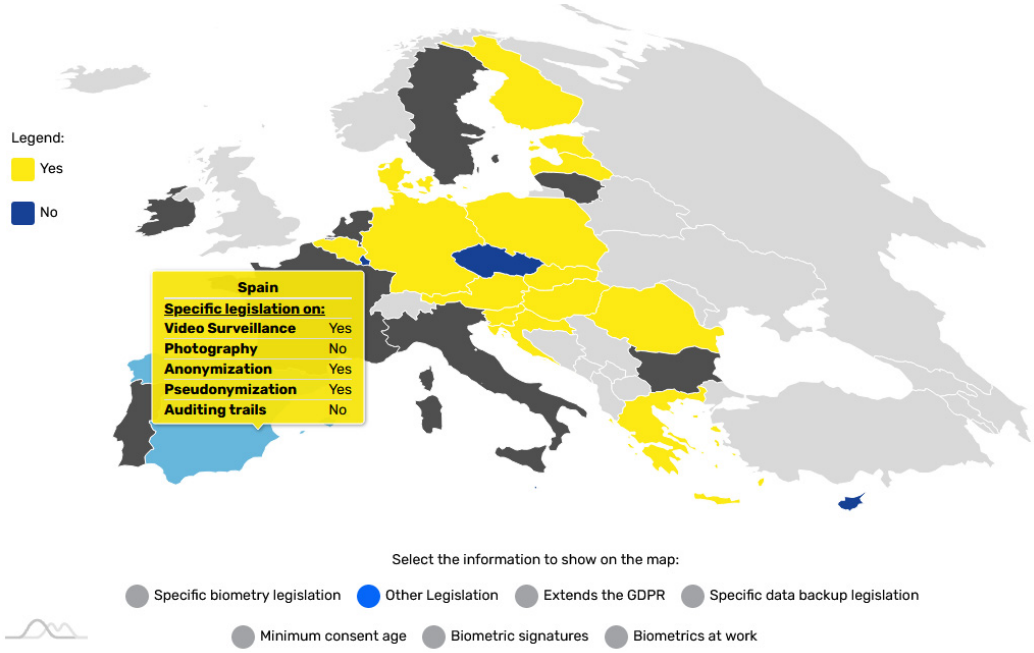

Figure 1. Map of data protection in EU, showing the additional legislation in Spain.

6. Conclusions

The GDPR privacy obligations for controllers and processors are rather extensive, and correctly implementing them takes a lot of time and work. Even if controllers and processors follow the prescribed procedures and take great care to ensure compliance, cross-border compliance challenges within the EU will persist. GDPR gives the EU member states certain leeway when it comes to data protection governance. These issues will manifest in the greater effort necessary for full GDPR compliance in all member states for cross-border service companies. This will impair service providers' overall efficiency in the Single European Market and cross-border competition in the member states.

The GDPR legislation gives the member states the flexibility to define or change specific aspects as they see fit. Member states can also always enact legislation that is stricter or has additional requirements than the GDPR. Not all member states, for example, allow biometrics to be used to obtain handwritten signatures. The use of biometrics for access control is also prohibited or restricted in some member states. As a result, services or products designed for one member state are only partially compatible with legislation in the other member states. Similarly, disparities in the minimum age for consent will necessitate service providers adapting their software and other solutions to account for differences between the member states. Though putting their software and other solutions in place may appear simple, understanding, collecting, and adhering to various regulations in all member states is not.

This paper collected and compared the legislation on data protection topics in the individual EU member states. The findings suggest that the member states do not have many additional/specific laws building on top of the GDPR. We discovered that additional or more specific laws are in place for only 29.4% of the cases discussed in this study.

Finally, we have developed a dynamic map, allowing for easy navigation among various information categories and comparisons of EU member states at a glance.

This research did have some limitations. The first limiting factor when wanting to collect data, as we have in this study, is that it is virtually impossible to collect it and check its validity by oneself. Because of the complexities involved (e.g., language barriers and learning about large amounts of legislation), the effort required would be too large without some external help. In return for relying on supervisory authorities, this workload is vastly reduced. Still, it also means we have to take whoever filled out the survey's word for it, and updating the information would require a repeated process of querying the supervisory authorities for the information. The other more obvious limitations are the missing EU member states that were not included in the study (because we were dependent on participation from supervisory authorities) and the limited number of topics we included in the survey. The last two limitations are also the basis for future work.

As such, in future work, we would like to extend the list of topics to discuss and compare between countries as well as include all of the EU member states missing in this study. Furthermore, we would like to delve into more detail for each of the topics by including lists of relevant national laws for each of the member states and potentially analysing them with the help of appropriate persons with adequate legal backgrounds from the respective countries.

Author Contributions: All authors equally contributed to the conception of the idea, the research plan's layout and participated in the literature search. M.H. led research activities, designed the conceptualisation, contributed to the investigation, defined and reviewed the methodology, performed the validation and designed as well as co-wrote the paper; B.K. performed the validation and co-wrote the original versions of the paper; M.K. contributed to the investigation, performed the validation and co-wrote the original paper. All authors equally contributed to the rest of the paper. All authors have read and agreed to the published version of the manuscript.

Funding: The authors acknowledge the financial support from the European Union's Horizon 2020 Research and Innovation Program under the CyberSec4Europe project (Grant Agreement No. 830929) and the Slovenian Research Agency (Research Core funding No. P2-0057).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). 2016. Available online: https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 11 October 2021).
2. United Nations Conference on Trade and Development. Data Protection and Privacy Legislation Worldwide. 2020. Available online: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed on 30 August 2021).
3. DLA Piper. Data Protection Laws of the World. Available online: https://www.dlapiperdataprotection.com/ (accessed on 30 August 2021).
4. i-Sight Software. A Practical Guide to Data Privacy Laws by Country. 5 March 2021. Available online: https://i-sight.com/resources/a-practical-guide-to-data-privacy-laws-by-country/ (accessed on 30 August 2021).
5. Park, S.; Akatyev, N.; Jang, Y.; Hwang, J.; Kim, D.; Yu, W.; Shin, H.; Han, C. A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. *Digit. Investig.* **2018**, *24*, S93–S100. [CrossRef]
6. Commission Nationale de l'Informatique et des Libertés CNIL. Data Protection around the world. 23 November 2020. Available online: https://www.cnil.fr/en/data-protection-around-the-world (accessed on 11 October 2021).

7. Long, W.; Blythe, F.; Member States' Derogations Undermine the GDPR. Privacy Laws & Business. May 2016. Available online: https://www.sidley.com/~{}/media/publications/gdpr-derogations.pdf (accessed on 19 August 2021).
8. Clearwater, A.; Philbrook, B. GDPR Derogations and How to Prepare for Member State Variation. *CPO Magazine*, 29 September 2017. Available online: https://www.cpomagazine.com/data-protection/gdpr-derogations-prepare-member-state-variation/ (accessed on 1 September 2021).
9. Vengadesan, J.; Pook, N. United with Differences: Key GDPR Derogations Across Europe. Penningtons Manches Cooper. 26 March 2019. Available online: https://www.penningtonslaw.com/news-publications/latest-news/2019/united-with-differences-key-gdpr-derogations-across-europe (accessed on 19 August 2021).
10. Custers, B.; Dechesne, F.; Sears, A.M.; Tani, T.; van der Hof, S. A comparison of data protection legislation and policies across the EU. *Comput. Law Secur. Rev.* **2018**, *34*, 234–243. [CrossRef]
11. activeMind.legal. Data Protection Comparison. Available online: https://www.activemind.legal/law/ (accessed on 19 August 2021).
12. Bird & Bird. GDPR Tracker. Available online: https://www.twobirds.com/en/in-focus/general-data-protection-regulation/gdpr-tracker (accessed on 30 August 2021).
13. Latham & Watkins. GDPR Derogations Tracker. April 2018. Available online: https://gdpr.lw.com/Home/Derogations (accessed on 30 August 2021).
14. Mutabazi, P. What is the Difference Between Digital Signatures and Electronic Signatures? LinkedIn. 23 May 2021. Available online: https://www.linkedin.com/pulse/what-difference-between-digital-signatures-electronic-mutabazi (accessed on 11 October 2021).
15. CyberSec4Europe—European Cybersecurity Competence Network. Available online: https://cybersec4europe.eu/ (accessed on 11 October 2021).
16. Heterogeneity of Data Protection Legislation across the EU, CyberSec4Europe. 9 September 2021. Available online: https://cybersec4europe.eu/heterogeneity-of-data-protection-legislation-in-the-eu/ (accessed on 11 October 2021).