Data Protection and Cybersecurity Certification Activities and Schemes in the Energy Sector

Iheanyi Nwankwo [1], Marc Stauch [1], Panagiotis Radoglou-Grammatikis [2], Panagiotis Sarigiannidis [2,*], George Lazaridis [3], Anastasios Drosou [3] and Dimitrios Tzovaras [3]

[1] Institute for Legal Informatics, Faculty of Law, Leibniz Universität Hannover, Konigsworther Platz 1, D-30167 Hannover, Germany; nwankwo@iri.uni-hannover.de (I.N.); stauch@iri.uni-hannover.de (M.S.)

[2] Department of Electrical and Computer Engineering, University of Western Macedonia, 50100 Kozani, Greece; pradoglou@uowm.gr

[3] Center for Research and Technology Hellas, Information Technologies Institute, 6th km Charilaou-Thermi Road, 57001 Thessaloniki, Greece; glazaridis@iti.gr (G.L.); drosou@iti.gr (A.D.); dimitrios.tzovaras@iti.gr (D.T.)

* Correspondence: psarigiannidis@uowm.gr

Abstract: Cybersecurity concerns have been at the forefront of regulatory reform in the European Union (EU) recently. One of the outcomes of these reforms is the introduction of certification schemes for information and communication technology (ICT) products, services and processes, as well as for data processing operations concerning personal data. These schemes aim to provide an avenue for consumers to assess the compliance posture of organisations concerning the privacy and security of ICT products, services and processes. They also present manufacturers, providers and data controllers with the opportunity to demonstrate compliance with regulatory requirements through a verifiable third-party assessment. As these certification schemes are being developed, various sectors, including the electrical power and energy sector, will need to access the impact on their operations and plan towards successful implementation. Relying on a doctrinal method, this paper identifies relevant EU legal instruments on data protection and cybersecurity certification and their interpretation in order to examine their potential impact when applying certification schemes within the Electrical Power and Energy System (EPES) domain. The result suggests that the EPES domain employs different technologies and services from diverse areas, which can result in the application of several certification schemes within its environment, including horizontal, technological and sector-specific schemes. This has the potential for creating a complex constellation of implementation models and would require careful design to avoid proliferation and disincentivising of stakeholders.

Keywords: certification; cybersecurity; data protection; energy

1. Introduction

With the advances in ICTs, various technical solutions have emerged to enhance the privacy and security of ICT products and services in various sectors. These privacy-enhancing and security functional properties found in many products and services are a welcomed development to forestall, or at least mitigate, the harm that could arise when devices and systems are compromised. There is, however, a level of uncertainty in the ecosystem because users and data subjects do not always have an objective way of verifying or assessing the assurance level of these technologies. In many instances, it is difficult to assess if the security controls in these products and services are implemented correctly or will operate as intended to meet the security challenges before they are deployed. Over the years, a complex system of certification has arisen globally, which aims to attest that these security functionalities are as they profess. Even so, in many cases, vulnerabilities in these components have exposed the systems in which they are deployed, causing them to be compromised.

Despite these shortcomings, the electricity sector has benefited immensely from the advances in ICTs. This is easily appreciated within the smart grid where these technologies have enabled a bidirectional flow of electricity and data, self-healing, and many other benefits, resulting not only in more efficient ways of analysing, reacting to and optimizing electricity demands but also in allowing electricity consumers to actively participate in the power supply system (prosumers) [1]. Within the grid ecosystem, several ICT-enabled components deployed in the power plants and substations have enabled better performance and advanced capabilities through the Internet of Things (IoT), advanced metering infrastructure, industrial automation and control systems and networking systems, among others. These components embed security functionalities given the critical roles they perform in the grid, and it is important that these security features are trustworthy and function as purported. Similarly, the personal data of consumers are processed in this bidirectional flow of data, raising the necessity that the privacy of these data subjects is protected throughout the lifecycle of this data processing.

Following the reforms in the EU data protection and cybersecurity laws, certification schemes have been introduced as a way for users to assess this security assurance level of products and services as well as the data protection compliance posture of the data controller. The adoption of the General Data Protection Regulation (GDPR) [2] and EU Cybersecurity Act (CSA) [3] which introduce certification schemes for personal data processing operation and ICT products, services and processes that incorporate a security functionality, respectively, are examples of EU policy implementation concerning privacy and cybersecurity. Since their introduction, several developments have occurred towards rolling out the various schemes as envisaged in these instruments, including the setting up of relevant frameworks by responsible agencies. For the data protection certification under the GDPR, for example, the data protection authorities have published a series of documents in a bid to establish the schemes [4,5]. The European Union Agency for Cybersecurity (ENISA), on the other hand, is setting up the various cybersecurity candidate schemes following the CSA.

Undoubtedly, these certification schemes will impact the industrial environment, particularly the energy sector where several automation systems include security functionalities, and personal data are processed in several customer-related operations such as consumer electricity provisioning. Industrial and automation control systems (IACS) deployed in substations, for instance, would benefit from secure components and products that are all certified to the appropriate assurance level, so as to avoid weak links that compromise the substations. Equally, it would be more protective for the electrical grid that highly involves sensor-intensive operations if the IoT technologies that regulate these sensors are certified, giving the assurance that they do not create security vulnerabilities. For power usage, the introduction of smart grids provides unique features such as load-demand balancing, dynamic pricing and demand-response by gathering fine-grained smart metering data from user households. The communication and network technologies used to send and receive data from the smart meters will be trusted if there are assurances through appropriate certification that they securely perform this function, protecting the confidentiality, integrity and availability of relevant data. This is especially important because, with the introduction of complex data analysis tools, it is now possible to extract individual energy consumption trends, which might reveal personal information regarding the occupants of a house.

Certification around the industrial environment is complex due to the different aspects of the protocols, architecture and components used within such environment. These include the information technology (IT) and operational technology (OT) environments and the many ICT products embedding security functionality, including supervisory control and data acquisition (SCADA), remote terminal unit (RTU), programmable logic controller (PLC) and more. The questions then are how best to harmonise the certification schemes for easy implementation and reuse and how to avoid a proliferation of certification in this environment. This paper shall identify the various developments in the certification schemes for

ICT products and services and personal data processing operations and analyse their impact in the EPES domain. Broadly, the paper contributes to the body of literature by providing a state of art on the regulatory development around data protection and cybersecurity certification schemes. It also recommends to stakeholders how to bridge the perceived gap in the framework. The remainder of the paper is structured as follows: Section 2 looks at related works, while Section 3 focuses on the materials and methods used to develop the paper. Section 4 contains the regulatory context of certification while Section 5 considers the data protection and cybersecurity certification requirements. Section 6 discusses the impact of these certification schemes in the EPES domain. Section 7 makes some recommendations to stakeholders, while Section 8 concludes the paper.

2. Related Work

Although many studies investigate the security and privacy issue with respect to EPES, such as [6–16], certification in the areas of data protection and cybersecurity is relatively new and, as such, only a few publications have focused on the regulatory aspects and the impact in an industrial environment such as the EPES domain. ENISA in [17] issued some recommendations with respect to data protection certification and in [18,19] regarding smart grid security certification. Following the adoption of the CSA, ENISA also published some documents in the area of certification including [20–22] and organised conferences on cybersecurity certification. Ad hoc working groups and stakeholder groups on cybersecurity have published relevant documents, including [23], on how to design the EU cybersecurity certification schemes. On their part, the European Data Protection Board (EDPB) has, in [4,5], given some guidelines on the establishment of the data protection certification scheme.

Other works have diverse focuses. For example, [24] tried to define the concept and methodology applicable to composite product evaluation using the smart cards and similar devices as a case study. Refs. [25–27] focused on the cybersecurity certification of IACS components and tried to lay down the groundwork for the development of a European IACS Components Cybersecurity Certification Scheme (ICCS). However, none of these works took a holistic and combined look at the regulatory developments stemming from the two most important EU legal instruments relating to data protection—the GDPR and cybersecurity—and the CSA, and none analysed their impact in the EPES domain. It is in this holistic approach that lies the main contribution of this paper.

3. Materials and Methods

A qualitative and descriptive doctrinal research method was adopted for this paper. Doctrinal research is a method of 'research which provides a systematic exposition of the rules governing a particular legal category, analyses the relationship between rules, explains areas of difficulty and, perhaps, predicts future developments' [28]. The doctrinal method involves a two-part process: first locating the sources of the law and then interpreting and analysing the text. In the first step, this paper identifies the laws requiring data protection and cybersecurity certification. In the second step, the provisions of the relevant laws are interpreted and analysed with the assistance of other primary and secondary sources on the subject, including technical materials. Primary data relied upon include EU secondary law and national legislation. Secondary materials were obtained from textbooks, journal articles, blogs, presentations, white papers, guidelines, opinions, media reports, EU reports and other relevant publications on the topics under study. As earlier indicated, this method differs from previous studies and methods by combining legal and technical methods in interpreting a regulatory framework that produces design and compliance effects in an industrial environment.

4. Regulatory Context

Certification is now part of the legal regime for data protection and cybersecurity within the EU. The key legal instrument in the field of data protection is the GDPR, which

includes several principles and requirements for data controllers and processors. These requirements, both obligatory and voluntary, form the current rules that allow a balancing of the society's needs for personal data processing and the data subjects' rights and freedoms. The GDPR also provides avenues for data controllers and processors to show accountability, transparency and compliance with these rules and a means for data subjects to evaluate these entities' compliance posture. Certification is one such avenue and falls within the realms of conformity assessment defined under Article 2 of Regulation No. 765/2008 as 'the process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled' [29]. Article 42 of the GDPR contains a voluntary certification framework for 'processing operation' involving personal data. This certification scheme relies on independent third-party evaluation and attestation. Although this certification scheme is voluntary, it could also be used to show the existence of appropriate safeguards in international data transfer.

However, the GDPR certification scheme under Article 42 has some limitations: it envisages that only data 'processing operations' can be certified as opposed to certification of devices and personnel. Secondly, the scheme is addressed to data controllers and processors as opposed to manufacturers and service providers who may be outside the category of data controller or processor. This means that a resort to other frameworks and schemes has to be made when intending to certify devices, systems or personnel for data protection compliance. If an EPES actor (as a data controller or process) wishes to certify its personal data processing operations as well as its products, devices or systems (as a manufacturer or provider), then the GDPR certification scheme will not be sufficient. A parallel certification scheme must be utilised that accommodates product, service and process certification.

The subsequently enacted CSA fills this gap to a large extent. It introduces a cybersecurity certification scheme for ICT products, services and processes within the digital single market, seeking to reduce the conflicting and overlapping national certification schemes on cybersecurity. Under the CSA, manufacturers and service providers can certify ICT products, services and processes that include a security functionality, and the Member States shall recognise such certification. The cybersecurity certification scheme will also assist users to assess the security assurance level associated with products, services and processes offered in the market. Like the GDPR, it is a voluntary scheme, at least until the European Commission designates some products, services or processes requiring mandatory certification [3].

The CSA interacts with the GDPR and other legislation in various ways. A crucial point of intersection and interoperability, arguably, lies in the fact that data security is an aspect of data protection principles and a requirement per Article 32 of the GDPR. Thus, cybersecurity certification could provide a vital element when assessing the security requirements during a data protection certification under the GDPR. In this case, there is a need to ensure a seamless application of both certification schemes. Directive EU 2016/1148 (Network and Information Security Directive (NISD)) [30] is another instrument that interacts with the CSA to the extent that it addresses critical infrastructure security such as energy, water, transport, health, digital infrastructure, banking and financial infrastructure and focuses on operators of essential services and digital service providers. The Directive incorporates cybersecurity and notification requirements for these operators. Although the NISD does not provide a certification scheme per se, a proposed Directive that will replace it—Directive on measures for a high common level of cybersecurity across the Union (NIS2)—contains a provision where the Member States may require essential and important entities to certify certain ICT products, services and processes under specific European cybersecurity certification schemes [31]. Further, Article 56 (3) of the CSA gives priority to the sectors identified as representing critical infrastructure under the NISD when the European Commission is assessing the cybersecurity certification schemes' efficiency. It is also notable that although the New Legislative Framework [32] aims to boost the quality of conformity assessments and enhance the credibility of the EC marking within the EU, it

does not explicitly address data protection and cybersecurity certification requirements. However, the framework complements the CSA and the GDPR by providing the rules for accrediting national accreditation bodies [29].

For the energy sector, other legal instruments may be relevant in terms of containing provisions related to data protection, cybersecurity or certification. These include Regulation 910/2014 (eIDAS Regulation) [33], requiring conformity of qualified electronic signature creation devices with specific requirements to ensure integrity and trust [33]. The Radio Equipment Directive 2014/53/EU (RED) [34], which requires manufacturers of radio equipment to ensure that such products do not harm the networks, incorporates safeguards to ensure personal data and privacy protection and support certain features ensuring protection from fraud [35]. This provision has formed a basis for a supplementary delegated regulation by the European Commission that applies these essential requirements to applicable radio equipment [35]. The proposed Directive on the resilience of critical entities, which aims to enhance the resilience of entities providing services essential for the maintenance of vital societal functions or economic activities within the EU's internal market, will also affect the energy sector concerning their cybersecurity resilience, although it has no certification provision [36].

Notably, implementation has started to occur in relation to the certification of some components in the energy sector. For example, the CEN/CENELEC/ETSI certification scheme for a harmonised European Protection Profile for Smart Meter Minimum Security requirements based on Common Criteria has been rolled out [37]. Moreover, at the national level, various laws provide for conformity assessment in the area of privacy and cybersecurity certifications, including those that aim at the certification of data protection officers or of data processing systems or those that focus on IT products' security, among others [38]. Overall, the EU is making significant efforts at reforming the cybersecurity landscape. A new cybersecurity strategy has recently been published [39], and a review of several instruments in this area is ongoing. In the proposed NIS2, for example, the European Commission shall be empowered to adopt delegated acts specifying which categories of essential entities must obtain a certificate per the European cybersecurity certification schemes [40]. This trend indicates that the cybersecurity landscape may involve mandatory horizontal requirements and certification in the future [41], and the EPES domain will be affected by such a mandatory scheme whenever these requirements are implemented.

With the impetus given to certification as a tool to demonstrate compliance within EU law, data controllers and processors, as well as manufacturers and service providers in the EPES domain, could leverage this tool to show greater transparency in their data processing operations on the one hand and enhance the security assurance level of their products, services and processes on the other hand. In the next section, the requirements of these certification schemes are discussed further.

5. Data Protection and Cybersecurity Certification Requirements

5.1. Requirements for Data Protection Certification under the GDPR

The GDPR applies whenever personal data are processed. Personal data have been defined in broad terms 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, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person' [2]. From this definition, a considerable amount of data processed in the energy sector could be regarded as personal data. When individual consumers, for example, enter into a contractual relationship with their energy providers, data are processed directly relating to these customers, such as their name and address, as well as indirect data that could be linked to them such as from the signatures in appliances processed in the smart meter hosted in their premises [42]. Operational data that directly or indirectly link to an

individual also fall within the scope of the GDPR's definition. Given such scenarios, specific data processing operations within the EPES domain could be certified under the GDPR.

The European Data Protection Board (EDPB) defines certification as 'third-party attestation related to processing operations by controllers and processors' [5], and Articles 42 and 43 of the GDPR provide the key procedural and substantive requirements for implementation. Apart from the above core provisions of Articles 42 and 43, the GDPR refers to certification in several other articles: Articles 24 (on the responsibility of data controllers); 25 (data protection by design and default); 28 (concerning data processors); 32 (on data security) and 46 (on data transfers). Essentially, certification may be used as an element of demonstrating compliance with the specific obligations contained in these articles [5]. It is also notable that the GDPR allows certification outside the scope of Articles 42 and 43, as can be seen by certification schemes targeted at Data Protection Officers (DPOs) or individuals, such as the one developed by the CNIL (French Supervisory Authority): certification scheme of DPO skills and knowledge [38].

The GDPR envisages that the data protection certification scheme may operate at two levels: the EU and national levels. Article 42 (5) requires that certification be based on approved criteria by the national supervisory authorities (SA) and/or national accreditation bodies or the EDPB (in the case of EU-wide data protection seals or marks). The procedure for the accreditation and functions of certification bodies is outlined in Article 43 and requires the competent SA and/or the national accreditation body to accredit certification bodies that possess the requisite expertise and fulfil certain conditions. These include demonstrating independence and expertise in relation to the subject matter of the certification; undertaking to respect the approved criteria; establishing procedures for the issuing, periodic review and withdrawal of data protection certification, seals and marks; establishing procedures and structures to handle complaints and demonstrating no conflicts of interest.

An entity wishing to act as a certification body can submit its certification criteria, as the case may be, to a national supervisory authority or the EDPB for approval. The EDPB has indicated possible topics that should be contained in such criteria such as the definition of data protection responsibilities, procedures and processing covered by the scope of the certification mechanism; relevant components of the processing operations (data, systems and processes); data protection principles; data subject rights; complaint handling framework; etc. [5]. Accreditation may be issued for a maximum of five years and may be renewed. It may also be withdrawn where the certification body no longer meets the conditions or infringes the GDPR. Additionally, Article 43 (5) requires certification bodies to provide the competent supervisory authority with the reasons for granting or withdrawing certification.

Apart from the requirements concerning accrediting the certification bodies, there are other substantive requirements associated with the actual certification process. These requirements are twofold: requirements stemming from the GDPR and those imposed by the certification bodies. On the one hand, the GDPR requirements are contained in the various principles and obligations that data controllers and processors must comply with, as indicated in several articles of the GDPR. For example, Article 5 contains the data protection principles, including lawfulness, transparency and fairness, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality and accountability. On the other hand, certification bodies may impose further requirements, such as payment of certification fees, completion of specific contracts, provision of certain information, allowing access, etc., before an applicant is certified.

It is essential to note the legal effect of certification: it does not relieve the affected entity of its obligations. As such, a certified entity must continue to comply with the Regulation. A postcertification breach of the GDPR requirements may lead to a withdrawal of the certificate. However, certification has a positive effect: it is one factor that supervisory authorities shall consider when imposing an administrative fine as per Article 83 of the

GDPR [5]. In this regard, obtaining certification could have a mitigating impact and affect the SA's opinion when deciding on fines.

Generally, any interested data controller or processor can then apply to the accredited certification body to undergo the process, preferably to the certification body of their choice, especially those located within their place of establishment. At the time of writing this paper, no certification body could be identified within the EU as having undergone accreditation based on the criteria contained in the GDPR. The SAs are still adopting their accreditation requirements, and a few have submitted their initial drafts to the EDPB for their opinion. The Luxembourg SA, for example, appears to have developed a 'GDPR—Certified Assurance Report based Processing Activities (CARPA) certification criteria (Version 1.0)' [43], which was subject of a recent EDPB opinion, although no certification has been carried out with these criteria yet. However, the UK's ICO has approved three certification schemes since it left the EU: ADISA ICT Asset Recovery Certification 8.0 [44], Age Check Certification Scheme (ACCS) [45] and Age Appropriate Design Certification Scheme (AADCS) [46]. The ICO has accredited Age Check Certification Services Ltd as the certification body for the ACCS [45] and AADCS schemes [46].

5.1.1. The Scope of Data Protection Certification

Under the GDPR, the object of certification is 'processing operations' by a data controller or processor. The EDPB has provided the core elements or components to be considered when assessing a processing operation. These are:

- Personal data (material scope of the GDPR);
- Technical systems—the infrastructure, such as hardware and software, used to process personal data;
- Processes and procedures related to the processing operation(s) [5].

To this end, processes involving personal data, such as collecting and storing personal data for service provision, transfer of data for processing, among others, can be certified under the GDPR and not the IT devices or systems per se. However, those tools form part of the assessment when evaluating the object of certification. The EDPB goes further to suggest four factors that can influence the assessment of each component: '(1) the organisation and legal structure of the controller or processor; (2) the department, environment and people involved in the processing operation(s); (3) the technical description of the elements to be assessed and (4) the IT infrastructure supporting the processing operation including operating systems, virtual systems, databases, authentication and authorisation systems, routers and firewalls, storage systems, communication infrastructure or Internet access and associated technical measures' [5].

Practically, the scope of certification under the GDPR could be general, involving multiple data processing operations within a data controller or processor environment, such as an online retailer's processing operation involving customer registration, advertisements, etc. Alternatively, it could be a specific target, in the sense of a particular aspect of processing, such as international data transfer. ENISA further clarifies that 'Art. 42(1) requires that a certification mechanism under GDPR must concern an activity of data processing. Such an activity may be (also an integral) part of a product, a system, or service, but the certification must be granted in relation to the processing activit(ies), and not to the product, system or service as such (e.g., certification of data deletion process in product X)' [17]. This statement shows that privacy-related certification for products alone, or services and processes targeting manufacturers, is outside the scope of Article 42 of the GDPR. As earlier alluded to, the aspect relating to a product's cybersecurity is covered within the CSA's certification framework. The extent of complementarity of both schemes, as earlier noted, lies in the fact that data security is an aspect of data protection. As such, a cybersecurity certification that covers a relevant security measure envisaged under the GDPR could be used as evidence when undergoing a data protection certification to demonstrate compliance within such an aspect of data security.

5.1.2. Postcertification Compliance under the GDPR

Certification may be issued for a maximum of three years, which is renewable. A postcertification surveillance regime is envisaged under the GDPR. During this period, the certified entity must continue to comply with the rules. Simultaneously, the certification body and supervisory authority shall continue to monitor the entity's compliance with certification criteria. Noncompliance at this stage may lead to a revocation of the certificate by the certification body or SA before the end of the term initially indicated.

5.2. Requirements for Cybersecurity Certification under the CSA

Any ICT product, service or process that contains a security functionality, in general, qualifies for certification under the CSA. The CSA allows two assessment approaches when assessing ICT products, services and processes: a self-assessment and a third-party assessment. Article 53 of the CSA recognises a conformity self-assessment under the sole responsibility of the manufacturer or provider of ICT products, services or processes. Such conformity self-assessment applies only in relation to ICT products, services and processes that present a low risk corresponding to assurance level 'basic' (which is evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks). Performing a self-assessment takes the form of a manufacturer collecting, documenting and maintaining any necessary evidence related to the ICT product, service or process and using this evidence to evaluate the conformity of the product, service or process against the criteria for the assurance level 'basic', as applicable to such a product, service or process. This evidence should be made available at any time for review by the National Cybersecurity Certification Authority (NCCA) of the competent Member State. Based on this evidence, the manufacturer may issue an EU Statement of Conformity for its product, service or process. The Statement of Conformity shall be submitted both to the NCCA and ENISA. ENISA maintains an overview of all the certificates and EU statements of conformity issued under the CSA.

On the other hand, an accredited independent conformity assessment body (CAB) performs a third-party assessment by evaluating the product against a defined set of criteria in the relevant scheme. There are three assurance levels recognised under Article 52 that could be obtained through a third-party certification: basic, substantial or high, which shall be commensurate with the level of the risk associated with the intended use of the ICT product, service or process, in terms of the probability and impact of an incident. The basic assurance level refers to the assurance level indicating that the ICT products, services and processes for which a certificate or EU statement of conformity is issued meet the corresponding security requirements, including security functionalities, evaluated at a level intended to minimise the known basic risks of incidents and cyberattacks. The evaluation activities to be undertaken shall include at least a review of technical documentation. The substantial assurance level refers to an assurance level indicating that the ICT products, services and processes for which a certificate is issued meet the corresponding security requirements, including security functionalities, evaluated at a level intended to minimise the known cybersecurity risks and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities and testing to demonstrate that the ICT products, ICT services or ICT processes correctly implement the necessary security functionalities. The high assurance level refers to the assurance level that the ICT products, services and processes for which a certificate is issued meet the corresponding security requirements, including security functionalities, evaluated at a level intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources. The evaluation activities to be undertaken shall include at least the following: a review to demonstrate the absence of publicly known vulnerabilities; testing to demonstrate that ICT products, services or processes correctly implement the necessary security functionalities as state-of-the-art and an assessment of their resistance to skilled attackers, using penetration testing.

A manufacturer or service provider who wishes to obtain this third-party certification shall apply to the appropriate CAB body and provide evidence supporting the security assurance level it seeks to confirm. The CAB (evaluator) then reviews this evidence and conducts applicable conformity assessment activities (design review, source code review, security functional testing, penetration testing, etc.) and generates an evaluation report which will be reviewed by the CAB before deciding to grant a certificate if the requirements are satisfied [47]. A successful evaluation by the CAB results in the issuance of a certificate that attests the subject matter has been certified in accordance with a scheme and that it complies with the specified cybersecurity requirements and rules. The certificate shall also indicate the assurance level satisfied by the product and the criteria and methodology of evaluation.

The concrete requirements for evaluating ICT products, services or processes shall be contained in specific cybersecurity schemes, that is, a comprehensive set of rules, technical cybersecurity requirements, standards and evaluation procedures, defined at the EU level and published by ENISA [48]. Manufacturers, vendors, integrators and service providers that meet these requirements shall then apply to the appropriate conformity assessment body for certification. Applicants for certification shall also provide the required information, documentation and access to the CAB. So far, ENISA has developed the Common-Criteria-based European candidate cybersecurity certification scheme (EUCC) for the certification of ICT products, services or processes that meet the substantial and high assurance levels [20]. It has also worked towards establishing sector-specific schemes such as for cloud services [21] and 5G networks [49]. Recently, a Methodology for a Sectoral Cybersecurity Assessment was published by ENISA [22], and efforts are proceeding rapidly at finalising the above schemes. Under Article 49 (7), the European Commission has the responsibility of adopting an implementing act for a European cybersecurity certification scheme based on ENISA's work.

5.2.1. The Scope of Cybersecurity Certification

As already mentioned, the certification scheme under the CSA will cover ICT products, services and processes that contain security functionality. A report by the Stakeholder Cybersecurity Certification Group (SCCG) suggests that the future schemes may be grouped into three broad areas: horizontal, technological and sectoral schemes [23]. Table 1 indicates the possible scope of coverage of each scheme according to the SCCG report:

Table 1. Possible areas for future cybersecurity schemes according to the SCCG report.

Scheme Nature	ICT Products	ICT Services	ICT Processes
Horizontal scheme	Lightweight evaluation methodology	-	Security lifecycle, security by design (incl. patch management)
Horizontal scheme	Full evaluation of IT products	-	ISMS
Horizontal scheme	Protection profiles evaluation	-	Supply chain security: vendor security assessments
Horizontal scheme	Cryptographic evaluation	-	Secure software development (DevOps, Agile, waterfall products)
	Industrial components critical infrastructure	-	-

Table 1. *Cont.*

Scheme Nature	ICT Products	ICT Services	ICT Processes
Horizontal scheme	Composed systems evaluation	-	-
Technological scheme	5G network components	Security incident detection services	Network Equipment security (vendor process security)
Technological scheme	NESAS Products	Security incident response services	Assurance scheme (NESAS))
Technological scheme	5G customer equipment	Security design services	Cryptographic module /Algorithm validation scheme
Technological scheme	IoT (customer schemes and industrial scheme per sector for appliances, CCTV)	Security managed services	-
Technological scheme	eIDAS	Security audit services	-
Technological scheme	AI	eIDAS qualifies trust services	-
Technological scheme	Blockchain	IoT Services	-
Technological scheme	Consumer mobile device security evaluation	End-to-end evaluation related to end-user systems and services	-
Technological scheme	Consumer mobile device security evaluation	5G virtualisation services	-
Sectoral scheme	Industrial and automation control systems (and components)	Telco services supporting critical infrastructure	Road vehicle processes
Sectoral scheme	Road vehicle (transport: critical infrastructure)	-	-
Sectoral scheme	Railway system (transport: critical infrastructure)	-	-
Sectoral scheme	Areal and aviator systems (incl. drones) (transport: critical infrastructure)	-	-
Sectoral scheme	Medical devices	-	-
Sectoral scheme	Physical protection and fire protection installations	-	-
Sectoral scheme	Smart meters	-	-
Sectoral scheme	V2X communications	-	-

This table indicates both the initial cybersecurity certification scheme areas by the European Commission and the suggested additions by the SCCG. It is notable that the content of this table could be reviewed in future work by the European Commission, ENISA and the SCCG. Furthermore, the selection criteria for future schemes and criteria for prioritising schemes still need to be defined, and the level of the interdependence of the schemes must be ironed out, as well.

It is important to note that once the EU-level schemes are finalised, they may affect a lot of the national schemes. Thus, although efforts are being made to harmonise the two levels of the schemes, there is a possibility that some national schemes that are not following the EU schemes may be phased out or adjusted per the EU schemes.

5.2.2. Postcertification Compliance under the CSA

The holder of a European cybersecurity certificate shall inform the competent authority or conformity assessment body of any subsequently detected vulnerabilities or irregularities concerning the security of the certified ICT product, service or process that may impact its compliance with the requirements related to the certification. That authority or body shall forward that information without undue delay to the national cybersecurity certification authority concerned [3]. Violation of postcertification requirements may attract sanctions such as suspension or revocation of the certificate.

6. Discussion: Impact of Data Protection and Cybersecurity Certifications in the EPES Domain

6.1. Current Certification Landscape

Currently, certification schemes that focus on privacy and data protection are diverse: some target certification of personnel, while the others target products and processes. Notably, these schemes have been designed based on the GDPR and would need to be adjusted to reflect the GDPR requirements or replaced by a new GDPR framework. While these schemes may accommodate self-certification, the GDPR is entirely focused on third-party certification and, as such, there may be a need for data controllers and processors to have a precertification tool to self-assess their data processing operations to know if they are mature or fit for third-party certification. Such a tool would help them to check their compliance posture, identify gaps and improve their operations before applying for certification. Furthermore, while there are some sector-specific privacy certifications such as those targeted at cloud computing, there is no such sector-specific scheme for the EPES domain or a code of conduct. This will be highly valuable in the GDPR dispensation in order to have a more harmonised framework for this domain, including how sensitive documentation used for certification shall be protected.

Concerning cybersecurity certification, such initiatives are generally originated from the developers' and manufacturers' perspectives and are influenced by market analysis and users' requests, such as where certification is a requirement for public infrastructure. The certification process takes different stages: First, manufacturers analyse the market needs and decide which certification scheme to pursue. Such analysis would suggest the necessary standards and requirements to implement as well as the certification body to approach. Second, the certification procedure is initiated. In this stage, documentation, consultations and agreements are reached between the applicant and the certification body and testing facility where applicable. Thirdly, the evaluation proper is conducted by the certification body. During this process, further documentation and refinement may be requested, and if the evaluation is successful, the final part takes place, which is the issuance of the certificate and postcertification monitoring. Notably, certification is jurisdictionally limited. Only through a country's participation in the Common Criteria Recognition Arrangement (CCRA), the Senior Officials Group, Information Systems Security—Mutual Recognition Arrangement (SOGIS-MRA) or any other similar agreement can certificates issued be accepted and recognised by those participating countries. However, when the EU schemes are operative, aspects will change for any entity that wants to comply with the CSA; for example, the choice of certification body will be limited to those approved under the CSA. Furthermore, the EU schemes will provide specific requirements and standards for each scheme. One of the advantages of the EU-wide scheme will be that a certificate from any EU Member State shall be recognised by the other Member States, and there are possibilities that with appropriate agreement other countries outside will recognise these EU certificates. However, from a practical point of view, as could be deduced from the foregoing sections,

there could be potential complexity with the multiple schemes (generic, technological and sector-specific schemes) that is likely to emerge from the cybersecurity certification framework. While this could present several possibilities of certifying a product, it may also mean that several standards and requirements may apply to a component depending on the strand pursued by the manufacturer or developer. König et al. [50], for example, show that different standardization bodies, namely, the NIST, ANSI Accredited Standards Committee X9, ISO, the German Institute for Standardization (DIN), the ENISA, the German Federal Office for Information Security (BSI), the International Telecommunication Union (ITU) and the European Committee for Electrotechnical Standardization (CENELEC), are all working on standards in the area of blockchain. As such, there is a potential that overlap and duplication may arise, resulting in too many standards around a scheme involving blockchain technology. Thus, there is a need for a more harmonised and holistic approach to standardisation of requirements and interoperability of the future schemes, including reusing them where possible, particularly for new technology areas such as blockchain, 5G, IoT, etc.

6.2. Application of Multiple Certification Schemes

IACS products and components are developed by many manufacturers and suppliers scattered all over the globe. These components embed security functionalities including the SCADA systems that supervise industrial systems, the PLCs/IEDs (field process automation and control equipment), engineering/programming workstations for programming the field components of an IACS, databases used for process control and telecommunication systems, among others [51]. The application of these components in the energy domain has brought tremendous transformation in recent years, allowing for the seamless monitoring and transmission of data on power, water or gas usage as well as communicating information immediately from smart meters via linked sensors, thereby eliminating the need for providers to physically inspect installations to bill consumers and maintain the infrastructure. As a sector that employs different technologies and services from diverse areas, several certification schemes would be applicable within the EPES domain. This will involve schemes ranging from horizontal, technological and sector-specific schemes. For example, certifications that target smart meters and IACS used in the EPES domain may benefit from sector-specific schemes, which include specific protection profiles for the smart grid, while IoT and other network components may be subject to technological schemes. For their part, cryptographic evaluations and supply chain security may be issued from horizontal schemes. While such compartmentalisation may allow targeting of as many components as possible within an industrial environment, it could also lead to some complexity in a labyrinth of certifications within a single system, as shall be seen further in the next section.

6.3. Potential Complexity in the Constellations of Implementation Models

Certification in an industrial environment may take several shapes such as individual device certification, composite product certification, system/subsystem certification and process certification. Handling individual product certification may be easier due to the current knowledge base; however, composite products and systems may pose some complexity due to the interaction and integration of many devices in an operational environment, some of which may have different focuses and levels of security assurances. Given that the certification schemes are new and still emerging, the evaluation criteria for such a complex implementation model in the EPES domain would require a painstaking design to accommodate the complex environment in which they are to be implemented. Other challenges and questions in this respect relate to the lifecycle of the certificates: What will happen to the whole system certificate, for example, if one of the composite certificates is invalid or retracted by the certifying authority? Would any update to the system require a new certification? It is in light of these issues that clear guidelines would be necessary

from the authorities, including harmonising the relevant standards that would be necessary for these schemes.

6.4. Cost of Updating Existing Components and Recognition of Certification beyond the EU

There will be a cost and time associated with the certification schemes which at present remains difficult to ascertain. A challenge that manufacturers and developers may face is that when the new EU schemes are adopted, they would need to update their components to address specific requirements not yet covered for certification purposes. This may involve significant efforts and costs at upgrading existing components and systems to meet the requirements of the various EUCC schemes, particularly the legacy systems. An important lesson to learn from this is that it will be essential for product designers and manufacturers to henceforth consider certification requirements right from the beginning and throughout the security lifecycle, given that the URWP is subject to review every two years. This is significant because future developments of the URWP may include mandatory requirements, and putting such into consideration throughout the lifecycle of a product would allow for compliance with current and future requirements around a product. The value that stakeholders will acquire in return for the cost of engaging in the various schemes will potentially affect their enthusiasm for such schemes. This relates to another point, which is the scope of recognition of the certificates. Given that various stakeholders in the EPES domain have a global establishment, the scope of recognition of the EU certification scheme would incentivise stakeholders in adopting these certifications. Although the schemes are voluntary currently, the cost and business advantages of obtaining them present a huge opportunity for stakeholders in the energy sector to increase their global recognition if the EU certificates have a global reach.

6.5. Building Trust in the Ecosystem

Certifications would provide a level of reassurance that industrial products in the EU market are safe to a large extent. It will also offer users a less complex way of assessing the security assurance level associated with products, services and processes offered in the market. Although the certification framework under the GDPR and the CSA is of a voluntary character, stakeholders in the energy sector could leverage these schemes to increase trust and security for European consumers and businesses. Data protection certification, for example, would have an impact among the data subjects that interact with the smart grid, as several EPES sector activities involve the processing of customer data, ranging from energy usage data to billing. Certification offers an objective basis for assessing the compliance posture of the data controllers who are EPES stakeholders. There is a potential to reassure the public that EPES organisations take privacy and security seriously in their business and customer activities.

For ICT products and services, certification would assist in developing a competitive digital single market. It will not only support the security by design approach but also provide an avenue for ensuring regulatory compliance when stakeholders only purchase and integrate products and services with the required assurance level certificate. Customers may be expected increasingly to demand certification from manufacturers and service providers within the supply chain. This will create a business advantage for those who obtain the required certifications, as they would have access to the market. In this way, certification becomes an incentive, as it will affect participation in the common market.

6.6. Protection of the Documents Relating to Certification

Concerning documentation, a lot of effort will be involved in the entire process of certification, ranging from completing the application forms to generating technical documentation. Here, it is notable that business-sensitive and IP-related information will be involved, and this raises a concern as to how the certification bodies and the other actors involved in the certification framework such as the IT Security Evaluation Facility (ITSEF) would implement trusted mechanisms to protect this information. This is against

the backdrop that such actors may be subject to a freedom of information request and, if no confidentiality safeguards are in place, may lead to exposing sensitive information.

7. Recommendations

7.1. Recommendations Concerning GDPR-Focused Certification

7.1.1. Development of a Data Protection Precertification Tool

Given that data protection certification under the GDPR does not include a self-assessment conformity but only third-party assessment, the EDPB and SAs should develop a precertification tool that could help data controllers and processors first to evaluate their processing operation (a form of self-evaluation exercise). This precertification process would provide the possibility for intending applicants to selectively test their operations and requirements before engaging actual certification bodies. This tool could speed up the process and encourage controllers and processors to initiate certification processes.

7.1.2. Encouragement of a GDPR-Inspired Standard and EPES Sector-Specific Data Protection Certification Schemes

Stakeholders, including the EC, SAs, EDPB and European standards organisations should encourage and develop GDPR-inspired standards, which transpose GDPR provisions relevant for certification into technical requirements and specifications where applicable. This will ensure consistency of the benchmark and certification criteria and assist in bridging the gap in differences in interpretations given to the requirements. Engaging various stakeholders and disciplines, such as law, IT specialists, engineers, data protection authorities, etc., will be essential for this purpose. To complement the above, it is also essential to identify and harmonise existing relevant standards for all parts of data protection evaluation, such as DPIA, fair information principles and data security assessment. Due to data protection's multifaceted nature, aspects such as data security with more technical features can be aligned with standards in this area, such as ISO/IEC 27001 and ISO/IEC 15408. Mapping and harmonising these standards with a GDPR focus will help to provide greater clarity and consistency in future data protection certification schemes. In the long run, sector-specific data protection certification schemes should be encouraged and developed for the energy sector, since several data processing operations around the sector involve personal data. This could be augmented with a specific code of conduct around personal data processing for the sector (as encouraged under Article 42, GDPR). Such a sector-specific scheme should consider the specificities of personal data processing, actors and components/systems and data flow in this sector. This will make it attractive and easy for EPES actors to obtain such a certification.

7.1.3. Concretize Guidelines on the Certification Schemes

As lessons are learned from implementing the certification schemes, the relevant bodies such as the EDPB, Sas, NCCA and ENISA should regularly publish further guidelines and best practices on these schemes. Such guidelines should include aspects regarding the synergy between the data protection certification and cybersecurity certifications, as well as aspects regarding coherence in the various schemes that will be rolled out following the URWP. In this respect, for example, it is recommended that in future guidelines, clear examples be included on how the cybersecurity certification schemes can be relied upon to fill the gap that arose due to the limited application of the data protection certification framework. Furthermore, as the multiple schemes may breed complexities, concrete guidelines would help clarify (and avoid unnecessary duplication of effort) the overlapping and fragmented approaches and standards currently applied to different aspects of industrial certifications.

7.1.4. Protection of Certification Information

Another important recommendation that also applies to the CSA certification relates to the protection of the information provided by the data controller (or manufacturer/provider under the CSA) for the purpose of certification. Such information is sensitive, including both

data security and IP protected information, and it is recommended that a confidentiality framework be established around this information in the possession of the certification bodies and other actors that come in contact with it.

7.2. Recommendations Concerning CSA-Focused Certification

7.2.1. Adopt a Gradation Approach Concerning Certification of IACS Components and the Whole IACA System

When elaborating the various schemes that apply within an industrial environment, ENISA should consider the complexity that could arise between certification of IACS tools at the level of their individual components as opposed to the whole systems/subsystems level. This is partly a result of having components of varying assurance levels within a system. Other factors ranging from integration to maintenance may also pose specific challenges in a system certification scheme. In this respect, it is recommended to first focus on the component-level certification logically, where when all the components are secure the system will, to a large extent, reflect an assemblage of these components. Another reason why a component-level certification is preferred at this stage relates to changes in the components. Here it is relevant to consider what would happen to a system if one of the components is, for example, updated, or the certification is suspended or withdrawn: would the whole system assurance level change or should a new certification process be initiated to reflect the new state of the system? At a later stage, however, approaching certification at a system level should be the ultimate target, especially when the components have been tested over time and mature in their use. This way, the component-level certification can provide the building blocks and basis for a system-level certification.

7.2.2. Alignment of New Candidate Schemes with Existing National Schemes and to Make Room for Reuse of Certification

There are already existing national cybersecurity-related certification schemes; therefore, it is recommended that, where possible, ENISA should strive to align the new schemes with these existing ones to allow for a smooth transition to the new schemes as well as benefit those who are already familiar with the existing schemes. Furthermore, in the situation where one certification that covers a relevant aspect of another scheme can be reused, this should be encouraged, to retain the benefits in terms of cost and time needed for the process.

7.2.3. Identify Baseline Standards for Each Candidate Cybersecurity Certification Scheme

Similar to the recommendation for the GDPR scheme, standards that are relevant for each of the cybersecurity schemes should be identified and streamlined where possible to avoid duplication and overburden of standards. Standards do overlap in some areas, and, as such, there is a need for a baseline of standards for each cybersecurity certification scheme to ensure synergy and interoperability. This will assist developers and manufacturers in targeting the baseline requirements in their future developments amidst numerous global and regional standards. This will also be relevant for the composability of certification.

8. Conclusions

This paper has extensively analysed the EU data protection and cybersecurity certification frameworks stemming from two critical pieces of legislation that contain these schemes' requirements: the GDPR and the CSA. Although it is not obvious how these two schemes should be integrated in practice because both address different subject matter, this paper has noted the complementarity between the schemes in the area of data security, which is an aspect of data protection, while also being the primary focus of cybersecurity. Given the importance of cybersecurity, particularly within the industrial domain, certification would be frequently demanded by users as an essential tool to show compliance with the legal and technical requirements. While the EU certification schemes are currently voluntary, the trend may well move towards a mandatory approach, especially in critical and high-risk domains, such as the energy sector. Market demands may also force manufacturers and

service providers to adopt certification. However, there are possible challenges that may impact the smooth implementation of these schemes in the EPES domain. The complexity of the schemes needs to be addressed to facilitate easy adoption of certification. In addition, diversity of technologies and processes in such an industrial environment presents a challenge in certification, especially given that many legacy components are still used in this environment. This may have signification cost implications in updating exiting components to meet the certification requirements. It is also notable that certification constitutes no guarantee of cybersecurity. Postcertification compliance measures must be active, and stakeholders must be diligent in their engagements in the supply chain to achieve more holistic cybersecurity. Despite these challenges, certification presents a good avenue for manufacturers, developers, data controllers and processors to show their level of compliance. This will certainly have some comparative advantages for those who wish to participate in the EU single market and globally. In the light of the above discussion, some recommendations have been made to the stakeholders aimed at supporting and directing their attention when developing the schemes.

References

1. Panagiotis, R.G.; Sarigiannidis, P.; Dalamagkas, C.; Spyridis, Y.; Lagkas, T.; Efstathopoulos, G.; Sesis, A.; Pavon, I.L.; Burgos, R.T.; Diaz, R.; et al. SDN-Based Resilient Smart Grid: The SDN-microSENSE Architecture. *Digital* **2021**, *1*, 173–187.
2. European Parliament and Council of 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 10 February 2022).
3. European Parliament and Council of European Union. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act). 2019. Available online: https://eur-lex.europa.eu/eli/reg/2019/881/oj (accessed on 10 February 2022).
4. European Data Protection Board. EDPB Document on the Procedure for the Approval of Certification Criteria by the EDPB Resulting in a Common Certification, the European Data Protection Seal. 2020. Available online: https://edpb.europa.eu/sites/default/files/files/file1/edpbprocedureforeudataprotectionseal_postplencheck_en.pdf (accessed on 10 February 2022).
5. European Data Protection Board. Guidelines 1/2018 on Certification and Identifying Certification Criteria in Accordance with Articles 42 and 43 of the Regulation—Version Adopted after Public Consultation. 2018. Available online: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_en (accessed on 10 February 2022).
6. Radoglou-Grammatikis, P.; Sarigiannidis, P.; Iturbe, E.; Rios, E.; Martinez, S.; Sarigiannidis, A.; Eftathopoulos, G.; Spyridis, Y.; Sesis, A.; Vakakis, N.; et al. SPEAR SIEM: A Security Information and Event Management system for the Smart Grid. *Comput. Netw.* **2021**, *193*, 108008. [CrossRef]
7. Radoglou-Grammatikis, P.I.; Sarigiannidis, P.G. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. *IEEE Access* **2019**, *7*, 46595–46620. [CrossRef]
8. Zhang, H.; Liu, B.; Wu, H. Smart grid cyber-physical attack and defense: A review. *IEEE Access* **2021**, *9*, 29641–29659. [CrossRef]
9. Komninos, N.; Philippou, E.; Pitsillides, A. Survey in smart grid and smart home security: Issues, challenges and countermeasures. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1933–1954. [CrossRef]

10. Ghosal, A.; Conti, M. Key management systems for smart grid advanced metering infrastructure: A survey. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2831–2848. [CrossRef]

11. Kumar, P.; Lin, Y.; Bai, G.; Paverd, A.; Dong, J.S.; Martin, A. Smart grid metering networks: A survey on security, privacy and open research issues. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 2886–2927. [CrossRef]

12. Fan, Z.; Kulkarni, P.; Gormus, S.; Efthymiou, C.; Kalogridis, G.; Sooriyabandara, M.; Zhu, Z.; Lambotharan, S.; Chin, W.H. Smart grid communications: Overview of research challenges, solutions, and standardization activities. *IEEE Commun. Surv. Tutor.* **2012**, *15*, 21–38. [CrossRef]

13. Tan, S.; De, D.; Song, W.Z.; Yang, J.; Das, S.K. Survey of security advances in smart grid: A data driven approach. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 397–422. [CrossRef]

14. Asghar, M.R.; Dán, G.; Miorandi, D.; Chlamtac, I. Smart meter data privacy: A survey. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2820–2835. [CrossRef]

15. Moussa, B.; Debbabi, M.; Assi, C. Security assessment of time synchronization mechanisms for the smart grid. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1952–1973. [CrossRef]

16. Le, T.N.; Chin, W.L.; Chen, H.H. Standardization and security for smart grid communications based on cognitive radio technologies—A comprehensive survey. *IEEE Commun. Surv. Tutor.* **2016**, *19*, 423–445.

17. ENISA. Recommendations on European Data Protection Certification. 2017. Available online: https://www.enisa.europa.eu/publications/recommendations-on-european-data-protection-certification (accessed on 10 February 2022).

18. ENISA. Smart Grid Security Certification in Europe. 2014. Available online: https://www.enisa.europa.eu/publications/smart-grid-security-certification-in-europe (accessed on 10 February 2022).

19. ENISA. ENISA Smart Grid Security Recommendations. 2012. Available online: https://www.enisa.europa.eu/publications/ENISA-smart-grid-security-recommendations (accessed on 10 February 2022).

20. ENISA. Cybersecurity Certification: Candidate EUCC Scheme. 2020. Available online: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme (accessed on 10 February 2022).

21. ENISA. EUCS—Cloud Services Scheme. 2020. Available online: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme (accessed on 10 February 2022).

22. ENISA. Methodology for Sectoral Cybersecurity Assessments. 2021. Available online: https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment (accessed on 10 February 2022).

23. ENISA. EU Cybersecurity: A Newly-Formed Stakeholders Group Will Work on the Cybersecurity Certification Framework. 2020. Available online: https://www.enisa.europa.eu/news/enisa-news/first-meeting-of-the-stakeholders-cybersecurity-certification-group-sccg (accessed on 10 February 2022).

24. Joint Interpretation Library. Composite Product Evaluation for Smart Cards and Similar Devices. 2018. Available online: https://www.sogis.eu/documents/cc/domains/sc/JIL-Composite-product-evaluation-for-Smart-Cards-and-similar-devices-v1.5.1.pdf (accessed on 10 February 2022).

25. Paul, T. *Introduction to the European IACS Components Cybersecurity Certification Framework (ICCF): Feasibility Study and Initial Recommendations for the European Commission and Professional Users*; Technical Guidance KJ-01-17-099-EN-N; Joint Research Centre: Ispra, Italy, 2016. [CrossRef]

26. Theron, P.; Lazari, A. *The IACS Cybersecurity Certification Framework (ICCF). Lessons from the 2017 Study of the State of the Art*; Technical Report KJ-NA-29237-EN-N; Joint Research Centre: Luxembourg, 2018. [CrossRef]

27. Paul, T.; Francisco, R.G.J.; Tony, B.; Jean-Michel, B.; Roberto, C.; Luis, F.; Matthew, F.; Sergio, G.; Janusz, G.; Tiziano, I.; et al. Proposals from the ERNCIP Thematic Group, "Case Studies for the Cyber-Security of Industrial Automation and Control Systems", for a European IACS Components Cyber-Security Compliance and Certification Scheme. 2020. Available online: https://erncip-project.jrc.ec.europa.eu/documents/proposals-erncip-thematic-group-case-studies-cyber-security-industrial-automation-and-0 (accessed on 10 February 2022).

28. Hutchinson, T.; Duncan, N. Defining and describing what we do: Doctrinal legal research. *Deakin L. Rev.* **2012**, *17*, 83. [CrossRef]

29. European Parliament and Council of European Union. Regulation (EC) No 765/2008 of the European Parliament and of the Council of 9 July 2008 Setting out the Requirements for Accreditation and Market Surveillance Relating to the Marketing of Products and Repealing Regulation (EEC) No 339/93. 2008. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008R0765 (accessed on 10 February 2022).

30. European Parliament and Council of European Union. 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. 2016. Available online: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (accessed on 10 February 2022).

31. European Parliament and Council of 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 (EU) 2016/1148. 2020. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2020%3A823%3AFIN (accessed on 10 February 2022).

32. European Commission. New Legislative Framework. Available online: https://ec.europa.eu/growth/single-market/goods/new-legislative-framework_en (accessed on 10 February 2022).

33. European Parliament and Council of European Union. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and

Repealing Directive 1999/93/EC. 2014. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG (accessed on 10 February 2022).

34. European Parliament and Council of European Union. Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the Harmonisation of the Laws of the Member States Relating to the Making Available on the Market of Radio Equipment and Repealing Directive 1999/5/EC. 2014. Available online: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32014L0053 (accessed on 10 February 2022).

35. European Parliament and Council of European Union. Commission Delegated Regulation (EU). . . /. . . Supplementing Directive 2014/53/EU of the European Parliament and of the Council with Regard to the Application of the Essential Requirements Referred to in Article 3(3), Points (d), (e) and (f), of that Directive C/2021/7672 Final. 2021. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM%3AC%282021%297672&qid=1638116539090 (accessed on 10 February 2022).

36. European Parliament and Council of European Union. Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities COM/2020/829 Final. 2020. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN (accessed on 10 February 2022).

37. Volkwyn, C. Europe: First Harmonised Approach for Security Certification of Smart Meters Has Been Formally Certified. 2019. Available online: https://www.smart-energy.com/industry-sectors/smart-meters/europe-first-harmonised-approach-for-security-certification-of-smart-meters-has-been-formally-certified/ (accessed on 10 February 2022).

38. Commission Nationale de lÍnformatique et des Libertés. CNIL Certification Scheme of DPO Skills and Knowledge. 2019. Available online: https://www.cnil.fr/sites/default/files/atoms/files/cnil_certification-scheme-dpo-skills-and-knowledge.pdf (accessed on 10 February 2022).

39. European Parliament and Council of European Union. Joint Communication to the European Parliament and the Council the EU's Cybersecurity Strategy for the Digital Decade JOIN/2020/18 Final. 2020. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN:2020:18:FIN (accessed on 10 February 2022).

40. European Parliament. The NIS2 Directive: A High Common Level of Cybersecurity in the EU. 2021. Available online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689333/EPRS_BRI(2021)689333_EN.pdf (accessed on 10 February 2022).

41. Matheu, S.N.; Hernández-Ramos, J.L.; Skarmeta, A.F.; Baldini, G. A survey of cybersecurity certification for the Internet of Things. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–36. [CrossRef]

42. Finster, S.; Baumgart, I. Privacy-aware smart metering: A survey. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1088–1101. [CrossRef]

43. Commission Nationale pour la Protection des Données. GDPR-Certified Assurance Report Based Processing Activities Certification Criteria V1.0. 2018. Available online: https://cnpd.public.lu/dam-assets/fr/professionnels/certification/GDPR-CARPA-Criteria-for-certification-v10.pdf (accessed on 10 February 2022).

44. UK Information Commissioner's Office. ADISA ICT Asset Recovery Certification 8.0. 2021. Available online: https://ico.org.uk/for-organisations/adisa-ict-asset-recovery-certification-80.

45. UK Information Commissioner's Office. Age Check Certification Scheme (ACCS). 2021. Available online: https://ico.org.uk/for-organisations/age-check-certification-scheme-accs/ (accessed on 10 February 2022).

46. UK Information Commissioner's Office. Age Appropriate Design Certification Scheme (AADCS). 2021. Available online: https://ico.org.uk/for-organisations/age-appropriate-design-certification-scheme-aadcs/ (accessed on 10 February 2022).

47. ENISA. Standardisation in Support of the Cybersecurity Certification. 2020. Available online: https://www.enisa.europa.eu/publications/recommendations-for-european-standardisation-in-relation-to-csa-i (accessed on 10 February 2022).

48. ENISA. Certification Schemes and CABs—FAQ. 2021. Available online: https://www.enisa.europa.eu/topics/standards/certification/certification-schemes-and-cabs (accessed on 10 February 2022).

49. ENISA. Securing EU's Vision on 5G: Cybersecurity Certification. 2021. Available online: https://www.enisa.europa.eu/news/enisa-news/securing_eu_vision_on_5g_cybersecurity_certification (accessed on 10 February 2022).

50. König, L.; Korobeinikova, Y.; Tjoa, S.; Kieseberg, P. Comparing blockchain standards and recommendations. *Future Internet* **2020**, *12*, 222. [CrossRef]

51. Theron, P.; Bologna, S. Case Studies for the Cyber-Security of Industrial Automation and Control Systems. 2014. Available online: https://erncip-project.jrc.ec.europa.eu/sites/default/files/2015_1441_src_en_pth-erncip-iacsreport-201411-at-accepted_pth2-op.pdf (accessed on 10 February 2022).