IRSTI 06.51.25 https://doi.org/10.26577/FJSS.2023.v9.i1.09

THE EUROPEAN DATA PROTECTION MODEL AS A GLOBAL PRIVACY STANDARD

S.B. Akhmetova * , **A.S. Ibrayeva**
Al-Farabi Kazakh National University, Almaty, Kazakhstan
*e-mail: akhmetova.saule@gmail.com

Abstract. Discussions about generally accepted rules for personal data protection began in the 1970s, and in the early 1980s, the first international instruments appeared. Modern information technologies and cross-border data exchange have led to a discussion of the need to harmonize national laws for personal data protection.

This article discusses international instruments for protecting personal data and the works of foreign scholars. The purpose of the study is to analyze international instruments and identify common positions, characteristics and differences. The practical value of the article lies in the fact that it allows us to understand the desire of countries to harmonize their national data protection regimes. The scientific relevance lies in that the existing international legal norms and approaches to regulating personal data protection outside of Kazakhstan have yet to be studied in Kazakhstani legal science. The discussions presented in this article are of scientific and practical interest to undergraduate, graduate and doctoral students.

General scientific and particular research methods were used to prepare the study. The normative basis of the study was the OECD Guidelines, Convention 108, UN Guidelines, APEC Framework, DPD, and the GDPR. The theoretical basis is the publications of well-known foreign scholars in the field of privacy, such authors as Graham Greenleaf, Christopher Kuner, Priscilla Regan, Anu Bradford, Colin Bennett and others.

As a result of the study, it was concluded that most foreign authors recognize the European data protection model as a globally recognized standard being implemented in many countries.

Key words: privacy, personal data, GDPR, Convention 108, APEC Framework, OECD Guidelines, UN Guidelines, Directive 95/46/EC.

Introduction

Data protection was conceived after World War II and was driven by increased surveillance during the communist post-war era. Discussions about a generally accepted standard for protecting personal data began in the 1970s. In the early 1980s, the first international instruments, namely the OECD Guidelines and Convention 108, appeared concerning the regulation of international data transfer.

The rules governing personal data protection on the Internet were developed decades before the first tablets, smartphones, social networks or e-commerce were created or used. However, new technological developments have led to other problems in the modern networked information society in protecting personal privacy and freedom that the existing data protection rules cannot solve.

Modern technologies and business models, in particular cloud computing and location-based services, greatly impacted the transborder personal data flows at national and international levels. The globalization of socio-economic and political relations, the introduction of information and Internet technologies in international trade and interstate data exchange led to a discussion of the existence or need to develop a single international regulatory standard for protecting personal data. De Hert and Papakonstantinou note that contemporary global and complex personal data processing makes international data privacy governance more necessary than ever (De Hert and Papakonstantinou 2013: 274). The OECD Guidelines, Convention 108, the UN Guidelines, the Asia-Pacific Economic Cooperation Framework (APEC Framework), the Directive 95/46/EC (Data Protection Directive or DPD), and its successor, the GDPR, are most frequently discussed in the academic literature as an international instrument governing privacy. Opinions differ among authors regarding which of the listed legal instruments can be recognized as the gold or global standard for privacy protection.

 © 2023 al-Farabi Kazakh National University

Problem statement

Privacy laws vary widely across the globe in scope and strength of regulation. With the development of the Internet and information technology, the increased data exchange between commercial and government agencies has led to changes in existing and the formation of new national privacy laws. Moreover, in connection with the current cross-border data flow in the context of global trade, the need for harmonization of national laws or the existence of generally accepted international rules is becoming increasingly important.

Legislation in some countries has been influenced by the Fair Information Principles (or FIP), implemented as a global model in the OECD Guidelines with non-binding character. The Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) also establish a global understanding of the right to respect private life as a constitutional norm. However, implementing the constitutional norm by special laws on the confidentiality of information in individual countries has similarities and differences.

The EU aimed to protect EU citizens' personal data when processed outside the EU. The European data protection regime restricts the export of personal data from the EU to countries that do not have the same degree of privacy protection as in Europe (adequacy requirement). Despite allegations of extraterritorial action, this data export requirement has encouraged non-EU legal systems to enact laws like the DPD. For this reason, some scholars see the European regime as the gold standard or global model for protecting personal data.

However, more countries have or are implementing rules similar to data protection in Europe. The incentive is often the desire to secure revenue streams from EU companies and consumers. In other words, the national legislation of non-European countries is influenced by an external force and not by the presence of an internal priority of confidentiality.

The countries of the South American and African continents are building their own privacy rules that are more part of the constitutional privacy regime, have more general constitutional guarantees, a lack of detail, and a vague constitutional statement. In other words, South American and African states do not have any general confidentiality regimes.

Following the OECD Guidelines, the APEC Framework has been adopted for countries in the Asia-Pacific region, which attempts to establish common privacy protection principles for APEC countries. However, can the regional APEC Framework be considered a global legal model?

There is not comprehensive privacy law in America like in the EU. The US data protection regime is fragmented, sectoral, and in some critical cases, supported by soft rather than imperative legislation. For this reason, the US privacy regime did not meet EU adequacy requirements, and US companies had legal problems. However, some privacy issues are more effective in the US than Europe. Nevertheless, the US data protection model can hardly be considered a global one.

The UN Guidlines are seen as another tool for global data protection. Considering that the UN is essentially an international organization, it is evident that the UN's Guidelines should have been implemented on all continents. However, this did not happen due to their voluntary nature. Nevertheless, the UN Guidlines have influenced the widespread adoption of privacy principles worldwide.

Research question

Globalization of economic and socio-political relations is becoming inevitable for all countries. Information technologies penetrate deeper into all social and interstate relations, exacerbating the risks to human rights. One way or another, exchanging data at the interstate level or in the commercial sector has become a reality and a necessity in every country.

In the context of different legal systems and existing international instruments in the field of privacy protection, is there a regulation followed or recognized globally as a model framework that unifies different approaches?

Purpose of the study

This article will consider the views of scientists on international agreements governing the protection of personal data. This article aims to conduct a comparative analysis of international instruments and works of foreign authors to identify common positions, characteristics and differences in their conclusions. The practical value of the article lies in the fact that it allows us to understand the desire of the world community to harmonize the legal regime for the protection of personal data to establish mutually applicable rules for the protection of personal data, thereby bringing national laws closer together. The scientific relevance lies in the fact that the existing international legal norms and approaches to regulating personal data protection outside of Kazakhstan have been little studied in Kazakhstani legal science. The discussions presented in this article are of scien-

tific and practical interest to undergraduate, graduate, and doctoral students.

Materials and methods

General scientific, general and particular research methods were used to prepare the study. The normative basis of the study was international legal acts, in particular the OECD Guidelines, Convention 108, the UN Guidelines, the Asia-Pacific Economic Cooperation Framework (APEC Framework), the former Directive 95/46/EC (DPD), and the GDPR. Functional and comparative analysis of these international documents was carried out, and their provisions were studied, compared and analyzed. The normative comparison shows similarities and differences in the approach to protecting personal data, the legal force of international instruments and their mandatory implementation at the national level.

The theoretical basis is the publications of well-known foreign lawyers in the field of privacy, such authors as Graham Greenleaf, Christopher Kuner, Alessandro Mantelero, Paul de Hert, Vagelis Papakonstantinou, Priscilla Regan, Anu Bradford, Colin Bennett and others.

Results and discussions

In this section, we consider the OECD Guidelines, Convention 108, UN Guidelines, APEC Framework, Directive 95/46/EC, and the GDPR and opinions of well-known foreign scholars in the field of privacy about international privacy regulations.

OECD Guidelines

OECD Guidelines state basic principles of data protection: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation (which includes access to data and correction), and accountability. Greenleaf notes them as 'global elements common to four international instruments' (Greenleaf 2012: 73), meaning the OECD Guidelines, Convention 108, APEC Framework, and DPD. OECD Guidelines also provide the free flow and legitimate restrictions for transborder data flow.

However, the OECD Guidelines are not legally binding, and member states are recommended to consider them in their domestic legislation. Many scholars note this recommendatory feature of the OECD Guidelines. For example, according to Greenleaf (2013: 11), the very title of the OECD document implies that they are just guidelines, 'they have no legal effect anywhere'. Sunni Yuen thinks that OECD data protection principles are 'not strong' but were 'the foundation of the DPD' which was adopted by the EU in 1995 (Yuen 2007-2008: 63). Kuner (Kuner 2009: 314) also believes that the OECD recommendations influenced the content of national laws and other international instruments, but at the same time were not legally binding.

Probably the OECD Guidelines themselves did not aim to be binding. Perhaps they intended to set up a consensus about fundamental fair principles that could be the "first step" for subsequent binding international agreements (paragraph 8 of the Explanatory Memorandum to the OECD Guidelines). Paragraphs 14 and 20 of the Explanatory Memorandum to the OECD Guidelines refer to Convention 108, which was adopted by the Committee of Ministers of the Council of Europe on 17 September 1980 and was to be legally binding on its Parties.

Convention 108

In academic literature, Convention 108 has more admission as an international framework for data protection because of its binding nature compared to OECD Guidelines. Convention's Article 4.1 obliges the Parties to take measures in domestic law to give effect to basic principles for data protection.

In addition, Convention 108 (Articles 10 and 12.2) about sanctions and transborder data flow is more straightforward than the respective provisions of OECD Guidelines (paragraphs 19 and 17). The adequacy criterion for the exchange of personal data between signatory states to Convention No. 108 has become one of the most critical official provisions for the first time, according to De Hert and Papakonstantinou (de Hert and Papakonstantinou 2014: 633).

Also, Convention 108 is open for accession by non-members of the Council of Europe (Article 23). That means Convention 108 could be an international agreement and spread the core privacy principles beyond the European borders. Kuner (Kuner 2009: 313) views the Convention as having potentially a 'universal' application, i.e., proving the basis for global data protection standards. In his view, Convention 108 already contains an international treaty-based data protection framework (Kuner 2014: 66). His position is supported by Graham Greenleaf, who characterizes the Convention as a key instrument of global governance of privacy which has no realistic competitors» (Greenleaf 2012: 91).

De Hert and Papakonstantinou highlighted the reasons for the continued relevance of Convention

No. 108, adopted in 1981, in the mid-2010s (de Hert and Papakonstantinou 2014: 635). Firstly, it is the binding nature of Convention 108, despite the document's rather broad and flexible text. Secondly, persons covered by the provisions of Convention 108 on data processing were extended to public and private sector entities, including law enforcement agencies. Third, Convention 108, as a specialized instrument of the European Convention on Human Rights, further developed the implementation of Article 8 on privacy. In addition, Convention 108 allowed individuals to bring claims against governments and law enforcement agencies to an international court, the European Court of Human Rights in Strasbourg (ECtHR).

Nevertheless, the rhythms of technological development and global trade with increasing transborder data flow entailed amending Convention 108. In November 2001, the Additional Protocol to Convention 108 was opened for signature by its Parties. In 2012 the amendment process started and ended in May 2018 with the adoption of the modernized Convention 108+. Greenleaf marked the data protection principles of the revised Convention as 'very considerably stronger than those in the OECD Guidelines' (Greenleaf 2013: 5). The updated standards of Convention 108+ provide balanced protection of personal data globally. According to Greenleaf, the modernized provisions are "not too hot or too cold" but "just right" (Greenleaf 2013 : 12) to ensure that they eventually become globally accepted.

Mantelero tends to define the modernized Convention 108+ as a global standard for privacy rather than the new European Regulation, the GDPR (Mantelero 2021: 4). Differing data protection cultures, levels of maturity among services and service providers, and phases of the digital economy inevitably make the GDPR too ambitious a standard to be accepted everywhere. In addition, as an expression of the EU's regulatory policy, the GDPR is unlikely to be championed by its economic and political competitors.

Mantelero believes that the gold standard in the form of GDPR, whose provisions are not flexible but rather too strict, is challenging to implement in countries outside of Europe. In this case, it seems more feasible to develop a global standard, which could be Convention 108+ (Mantelero 2021: 4). Convention 108+ does not set the bar too high, but at the same time, it is the only international instrument capable of setting a threshold corresponding to the effective protection of human rights and freedoms and the effectiveness explicitly recognized in the GDPR (Mantelero 2021: 4). A striking example of this is the accession to the Convention of 108+ countries of the South American and African continents. To date, ten countries that are non-members of the Council of Europe have joined Convention 108.

UN Guidelines

According to de Hert and Papakonstantinou, the UN has distanced itself from the issues of international privacy regulation even though it has adopted the Guiding Principles, hosted international information society events, and has corresponding subdivsions (de Hert and Papakonstantinou 2013: 288).

There is not much support for voluntary UN Guidelines to be deemed a global data protection framework. For instance, Kuner notes that UN Guidelines' high-level data protection principles 'have been of limited practical relevance'(Kuner 2009: 313). However, he admits that the non-binding instruments of the UN and the OECD in the field of data protection have influenced laws worldwide (Kuner 2009 : 314). Birnhak also notes a cumulative effect of the OECD and UN Guidelines because they disseminated data protection principles and raised awareness around the globe (Birnhack 2008 : 512). However, Birnhak stresses the lack of binding force and the UN Guidelines' implementation procedures (Birnhack 2008: 511).

On the contrary, De Hert and Papakonstantinou note that UN guidelines have been unfairly underused. They point out UN Guidelines' advantages (de Hert and Papakonstantinou 2013: 321), particularly the absence of strict national or regional approaches compared to European instruments and the presence of the broadest possible range of recipients. In addition, the UN Principles are in line with human rights and address cross-border data transfer perspectives and adequacy issues. According to them (de Hert and Papakonstantinou 2013: 274), these principles could achieve international governance status and foster pervasive legislation, for instance, the same way as the IP, citing the Berne Convention as an example (de Hert and Papakonstantinou 2013: 274), which settled the fragmented approach of national laws to IP protection in the late 19th century. Following the example of the creation of a dedicated international body for the protection of IP (now WIPO), they recommend the creation of an international DPA at the UN that would administer the application of the existing UN Guiding Principles (de Hert and Papakonstantinou 2014: 635, de Hert and Papakonstantinou 2013: 320, 321).

APEC Framework

APEC (Asia-Pacific Economic Cooperation) includes 21 states, countries with strong domestic privacy traditions, such as New Zealand and Australia, and countries with minimal local privacy traditions, such as Taiwan, Vietnam, China and Thailand.

APEC Framework was adopted in 2005, a decade later than European DPD, which spread its 'adequate protection' principle to non-European countries by 2005. APEC Framework also did not find serious support to be recognized as a gold standard of data protection benchmark, mainly due to shortcomings such as the lack of rules for data storage, data export, and automated decision-making.

Sunni Yuen opines that the main reason lies in its 'aspirational rather than a binding framework' (Yuen 2007-2008: 60). She notes that a shortcoming of the APEC Framework is 'a large degree of discretion for firms to determine the appropriateness and need to comply with the principles of data protection (Yuen 2007-2008: 59). Keele also does not support APEC Framework because of its voluntary nature and the possibility of divergent implementation by national governments (Keele 2009: 365). De Hert and Papakonstantinou characterize APEC Framework as more flexible, with lower standard for data privacy protection (de Hert и Papakonstantinou 2013: 288). Phillips opines the APEC Privacy Framework has a voluntary regime with no independent legal effect (Phillips 2018: 526). Greenleaf notes 'that there are no APEC 'rules' at all, its Framework is a non-binding instrument, and APEC is not an international organization in the normal sense or even a treaty." (Greenleaf 2013: 11). Moreover, he noted that APEC would be seen as a dead-end because no one will follow non-binding rules (Greenleaf 2012: 80).

In contrast to many scholars, Kuner prefers the APEC approach to DPD's strict "adequacy requirements" because it is more flexible (Kuner 2009: 313). At the same time, Kuner notes that APEC Framework is more a regional rather than a global privacy instrument (Kuner 2014: 58).

Directive 95/46/EC

The European Convention on Human Rights and Convention 108 have been the foundation of European national data protection laws. However, due to the need for uniform application of these national laws, the DPD was adopted. Colin Bennet noted that the creation of the Directive was facilitated by the 'prior agreement on data protection principles within the OECD and the Council of Europe' (Bennett 2018: 244). However, these principles were enshrined more effectively by DPD. DPD 'cemented' 'adequacy requirement' for the transborder data transfer (Article 25), which entailed the diffusion and almost universal penetration of data protection principles (Philips 2018: 576). Many non-European countries had to align national privacy laws in conformity with DPD. Thus, the European regional privacy protection instrument spreading its provisions outside of Europe become a de facto global data protection standard.

In 1993 Regan described differences between US and EU perceptions of privacy and the approach to its protection, the need for harmonized global standards and comprehensive omnibus law in the US, and the establishment of supervisory data protection authority (Regan 1993: 257). She noted that the then-unadopted DPD probably would 'lead to a strengthening of US privacy' (Regan 1993: 267), which happened later.

For more than twenty years, DPD had a far greater global impact than thus far acknowledged and the main engine of the emerging data protection regime' (Birnhack 2008: 508). Birnhack notes that the directive was undoubtedly drawn up taking into account 'how third countries will react' (Birnhack 2008: 513). Moreover, this is what happened. For example, Yuen believes that the Directive's extra-territorial enforcement mechanism has made it the global standard (Yuen 2007-2008: 68, 82). Furthermore, she emphasizes that the reception of the DPD provisions from the standpoint of both practicality and efficiency allows for 'making the Directive a de facto global benchmark' (Yuen 2007-2008: 77).

Anu Bradford notes the "Brussels effect" on US companies doing business in Europe, which have been required to comply with the European Residents' Privacy Directive and have been sanctioned for violating it. The US is the leading e-commerce country on the planet. As such, many companies have had to adapt their Terms & Conditions and Privacy Policies to reflect European privacy regulations. Bradford argues that in many multinational companies, only the European privacy policy has company-wide application (Bradford 2012: 25). She notes that it is because of technical and economic non-divisibility of data and regulations, which require adequate data protection in all countries willing to interact with a sizeable and attractive EU market. 'Subscribing to EU rules is the price of trading with Europe' (Bradford 2012: 65).

Greenleaf describes ten global and ten European elements of DPD (Greenleaf 2012: 73,74,77). Many

elements can be found in many other national laws proving the DPD's global impact on data protection legislation.

Although most scholars tended to admit European Directive as a gold standard for regulating privacy globally, some disagreed. For instance, Kuner saw disadvantages of DPD because its extraterritorial application did not account for the law at the location of data processing properly (Kuner 2014: 64). He thought that any future global framework to be adopted should also address the rules about applicable domestic law (Kuner 2009: 313).

Although Rossi disagreed with treating DPD as a gold standard setter, he had a different opinion. While pointing out two strengths of DPD (establishing a supervisory authority and adequacy requirement), Rossi notes 'two loopholes' of DPD (Rossi 2014: 70, 71). The first is Article 25, allowing international agreements, for example, the EU-US Safe Harbour (Rossi 2014: 72). The second is Article 4 about the applicability of the national law, which can have weaker privacy protection than DPD, for instance, the Irish Safe Harbour (Rossi 2014: 74). According to Rossi, neither Europe nor governments set a global standard for Internet privacy but the companies (Rossi 2014: 77). He shares the opinion of Lessig and Rebecca MacKinnon that the software code regulates human behaviour almost in the same way as the law does (Rossi 2014: 76). Although the legal regulation can limit code regulation, the latter can 'constrain human behaviour in ways that are not foreseen in legal regulation, subverting it', for instance, through setting of defaults. How choices are structured and offered to us influences the decisions we make (Rossi 2014: 77).

GDPR

In response to historic challenges to privacy rights, data protection laws, including the EU Directive 95/46/EC (DPD), have evolved and expanded worldwide. Critical privacy threats that could not have been foreseen in the DPD emerged after its adoption, including the growth of the Internet, social media, online profiling and behavioral advertising, big data, and the Internet of Things. The European Parliament approved GDPR in April 2016, and on 25 May 2018, GDPR became effective. DPD had a substantive role in setting data privacy standards, and the GDPR 'was only possible because of twenty years of experience through the Directive' (Bennett 2018: 244). Thanks to more than twenty years of DPD implementation and the European case law about privacy, GDPR has become 'the most ambitious and comprehensive', 'multi-faceted instrument' which combines non-European 'policy instruments' (Bennett 2018: 242).

Many scholars treat GDPR as a global standard. Colin Bennet believes GDPR will impact on global protection of privacy because it, like DPD, 'will continue to offer an important template of principles and provisions for other jurisdictions' (Bennett 2018: 245). Butarelli considers GDPR as a setter of 'a genuine platform for global partnerships towards the 'global ubiquity' of data privacy' (Buttarelli 2016: 77). Cunningham McKay admits the EU 'extra-jurisdictional law', because the regional and national instruments do not fit effective regulation of data privacy on a global scale (McKay 2016: 449). Cedric Ryngaert & Mistale Taylor also believe GDPR is a worldwide standard (Ryngaert and Taylor 2020: 9).

Rustad and Koenig have the same opinion, noting that GDPR is 'a *bilateral synthesis of U.S. and EU privacy law'* (Rustad and Koenig 2019: 453). They mark GDPR as the basis of a worldwide "gold standard" for global data privacy' (Rustad and Koenig 2019: 366), but not purely European because 'much of the GDPR originated in U.S. law' (Rustad and Koenig 2019: 453). In their view, GDPR is a 'hybrid' EU and US instrument (Rustad and Koenig 2019: 412, 450, 453). Although many acknowledge the *'Brussels effect'*, they think there is also the '*D.C. Effect'* (Rustad and Koenig 2019: 365, 371, 412, 429). For instance, the GDPR took many US elements: 'long-established US tort concepts', Privacy by Design, wealth-based punishment, and security breach notification obligations' (Rustad and Koenig 2019: 368, 369, 371).

Paul Schwarz agrees with other scholars about the '*pathbreaking impact of EU privacy law* (Schwartz 2019: 776). In his opinion, most countries followed the European omnibus legal approaches 'due to their ease of enactment and comprehensiveness' (Schwartz 2019: 818). Even the US used the appealing 'EU-style data protection idea'. 'This phenomenon represents another way the EU has …reached important actors through the force of appealing ideas and a range of different kinds of interactions, which lead to a general process of acculturation to EU privacy concepts' (Schwartz 2019: 817).

Conclusion

The results of the study of scientific papers on international data protection instruments show that the OECD and UN guidelines have influenced the formation of the global legal regime but are not sup-

ported due to their voluntary nature and the lack of an implementation mechanism. The APEC Framework Convention is not regarded as a global standard due to its regional, non-binding and weak, albeit flexible, protection regime.

Although the European data protection model has been criticized, mainly by American scientists and politicians, it has confirmed its validity as a global standard. It has made a significant contribution to the development of legal data protection around the world. The adequacy requirement of Convention No. 108 and the DPD have extended data protection principles beyond Europe more effectively than non-binding OECD, UN and APEC guidelines. Strict requirements and oversight by data protection authorities have increased awareness of data subjects' rights. Moreover, the strict policies of the European Union have led to improvements in corporate regulations and privacy policies of companies, including prominent US companies (Schwartz 2019: 773). The enforcement of DPD by the European Court of Justice also significantly influenced data protection law.

Decades of DPD implementation and the *'DC effect'* played a significant role in shaping the provisions of the existing GDPR. GDPR does not need to be recognized as a gold standard in some official way or procedure. It is a '*the core of a de facto global policy standard'* (Rustad and Koenig 2019: 432).

However, given that GDPR is a regional instrument with an extraterritorial effect, it seems justifiable to agree with Graham Greenleaf that Convention 108+ as a short version of GDPR that allows other countries to accede to it could become more international and global 'in its ownership' (Greenleaf 2013: 11).

The strength of the European data protection model lies in its aim to protect all European individuals' fundamental rights and freedoms. Many scholars marked Europe's complex approach to safeguarding fundamental rights compared to the US's fragmented and sectoral privacy law. In addition, the basic principles of data protection received effectiveness through binding Convention 108, the establishment of data protection authorities and privacy law enforcement.

Europe is a multinational and multicultural region that cannot ignore different cultural contexts, legal frameworks and economic interests (Mantelero 2021: 4). That is why the European data protection model, formerly Convention 108 and DPD, and now the Modernized Convention 108+ and GDPR, reflect universal principles and standards for personal data protection, which make them globally recognized models, already implemented in many countries of the world, and which allow maximum converge and harmonize national laws.

References

APEC Privacy Framework (2005). Retrieved from https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf, accessed 30 April 2022

Bennett, C., (2018). The European General Data Protection Regulation: An Instrument for the Globalization of Privacy Standards?, 23(2) Information Polity: The International Journal of Government & Democracy in the Information Age, 239. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=bah&AN=130475522&authtype=shib&site=ehost-live&authtype=ip,shib&custid=ns075038, accessed 30 April 2022

Birnhack M. (2008). The EU Data Protection Directive: An engine of a global regime, 24(6), Computer Law & Security Review, 508. Retrieved from https://doi.org/10.1016/j.clsr.2008.09.001

Bradford, A. (2012). The Brussels Effect. Northwestern University Law Review, (2012)107(1), Northwestern University Law Review, 1. Retrieved from https://www.proquest.com/scholarly-journals/brussels-effect/docview/1286682884/se-2?accountid=14116, accessed 02 May 2022

Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard, 6(2) International Data Privacy Law, 77. Retrieved from https://doi.org/10.1093/idpl/ipw006, accessed 30 April 2022

Convention for the Protection of Human Rights and Fundamental Freedoms (the European Convention on Human Rights)

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.I.1981, (Convention 108). Retrieved from https://rm.coe.int/1680078b37, accessed 30 April 2022

De Hert P., Papakonstantinou V,'The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition', (2014)30(6) Computer Law & Security Review, 633. Retrieved from https://doi.org/10.1016/j.clsr.2014.09.002, accessed 30 April 2022

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: Implications for globalization of convention 108, 2(2), International Data Privacy Law, 68. Retrieved from https://www.proquest.com/scholarly-journals/influence-european-data-privacy-standards-outside/docview/1564000956/se-2?accountid=14116, accessed 30 April 2022

Greenleaf, G. (2013). Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?, 29(4), Computer Law & Security Review, UNSW Law Research Paper No. 2013-33, 11. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2262296, accessed 30 April 2022

Keele, B. (2009). Privacy by Deletion: The Need for a Global Data Deletion Principle, 16 Ind J Global Legal Stud 363. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/ijgls16&i=374, accessed 30 April 2022

Kuner, C. (2009). An International Legal Framework for Data Protection: Issues and Prospects, 25(4) The Computer Law and Security Report, 307. Retrieved from https://doi.org/10.1016/j.clsr.2009.05.001, accessed 30 April 30, 2022

Kuner, C. (2010). Data Protection Law and International Jurisdiction on the Internet (Part 1), 18(2) International Journal of Law and Information Technology, 176–193. Retrieved from https://doi.org/10.1093/ijlit/eaq002

Kuner, C. (2014). The European Union and the Search for an International Data Protection Framework, 2(2), Groningen Journal of International Law, 55, University of Cambridge Faculty of Law Research Paper No. 48/2015. Retrieved from http://dx.doi.org/10.2139/ssrn.2495273, accessed 30 April, 2022

Mantelero, A. (2021). The future of data protection: Gold standard vs. global standard, 40, Computer Law & Security Review. Retrieved from https://doi.org/10.1016/j.clsr.2020.105500, accessed 30 April 2022

McKa,y C. (2016). Complying with International Data Protection Law, 84 U Cin L Rev 421. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/ucinlr84&i=433, accessed 27 April 2022

Modernized Convention for the Protection of Individuals with Regard to Processing of Personal Data. Retrieved from https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1, accessed 02 May 2022

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Publishing, Paris. Retrieved from https://doi.org/10.1787/9789264196391-en, accessed 30 April 2022

Phillips, M. (2018). International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR), 137(8) Human Genetics, 575. Retrieved from link.gale.com/apps/doc/A553317905/AONE?u=ustrath&sid=bookmark-AONE&xid=6cba3a22, accessed 29 April 2022

Regan, P. (1993). The Globalization of Privacy: Implications of Recent Changes in Europe, 52(3) American Journal of Economics & Sociology, p257. Retrieved from https://search.ebscohost.com/login.aspx?direct=true&db=bah&AN=9308265340&authtype=shib&site=ehost-live&authtype=ip,shib&custid=ns075038, accessed 29 April 2022

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) OJ L 119/1.

Rossi, A. (2014). Internet Privacy: Who Sets the Global Standard?, The International Spectator,49:1, 65-80. Retrieved from https://doi.org/10.1080/03932729.2014.875823

Rustad M., Koenig,T. (2019). Towards a Global Data Privacy Standard, 71 Fla L Rev. Retrieved from http://www.floridalawreview.com/wp-content/uploads/Rustad-Koenig.pdf, accessed 30 April 2022

Schwartz, P. (2019). Global Data Privacy: The EU Way, 94 NYU L Rev771. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/nylr94&i=789, accessed 30 April 2022

UN Guidelines concerning Computerized Personal Data Files of 14 December 1990, UN Doc E/CN.4/1990/72, (UN Guidelines). Retrieved from https://www.refworld.org/pdfid/3ddcafaac.pdf, accessed 30 April 2022.

Yuen, S. (2008). Exporting Trust with Data: Audited Self-Regulation as a Solution to Cross-Border Data Transfer Protection Concerns in the Offshore Outsourcing Industry, 9 Colum Sci & Tech L Rev 41. Retrieved from https://heinonline.org/HOL/P?h=hein.journals/cstlr9&i=69, accessed 29 April 2022