universität wien

MASTER THESIS

Titel der Master Thesis / Title of the Master‘s Thesis

„The collision between data protection and data sharing in the EU and internationally “

verfasst von / submitted by

Sijana Fetibegovic

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Master of Laws (LL.M.)

Wien, 2022 / Vienna 2022

Studienkennzahl lt. Studienblatt / Postgraduate programme code as it appears on the student record sheet:	UA 992 548
Universitätslehrgang lt. Studienblatt / Postgraduate programme as it appears on the student record sheet:	Europäisches und Internationales Wirtschaftsrecht / European and International Business Law
Betreut von / Supervisor	Dipl.-Jur. Dr. Maria Sturm LL.M.

TABLE OF CONTENTS

ABSTRACT

Data sharing is a global phenomenon, that enables trade between countries, global competitiveness between data market players, as well as an increased partnership approach and cross-border initiatives to support technological innovation and social benefits. However, the advantages of data and cross-border data sharing are neither instantaneous nor are they equitably dispersed across and within countries. As such, data is a diverse asset whose value is defined by how it's used, with different implications for individuals, businesses, and governments. Many national regulations have been established to ensure that all data shared across borders receives the same degree of data protection, security, and privacy as data moves within the jurisdiction. According to the European Union, fundamental rights and values should serve as the cornerstone of data protection. Government data control is prioritised in the People's Republic of China as opposed to private sector data control in the United States of America. Furthermore, several governments have endorsed data localisation because of a lack of understanding of how data is handled on a global scale while adhering to applicable legislation. This thesis aims to examine whether data can be shared while being completely protected inside the European Union's member states and internationally. An overview of global trends and attitudes regarding data sharing and data protection among countries, individuals, and businesses will be given on the way to reaching the thesis's conclusion. Additionally, the complexity of data localisation will be highlighted in comparison to the many forms of data-sharing cooperation, such as open data, bilateral and plurilateral agreements, as well as numerous international arrangements aiming at establishing common standards.

Keywords: data sharing, data protection, cross-border, privacy, open data, restriction, data localisation

DEUTSCHER ABSTRACT

Die gemeinsame Nutzung von Daten ist ein globales Phänomen, das den Handel zwischen Ländern, die globale Wettbewerbsfähigkeit der Akteure auf dem Datenmarkt sowie einen verstärkten partnerschaftlichen Ansatz und grenzüberschreitende Initiativen zur Unterstützung technologischer Innovationen und sozialer Vorteile ermöglicht. Die Vorteile von Daten und grenzüberschreitendem Datenaustausch sind jedoch weder sofort verfügbar, noch sind sie gleichmäßig über und innerhalb der Länder verteilt. Daher sind Daten ein vielfältiges Gut, dessen Wert davon bestimmt wird, wie es verwendet wird, mit unterschiedlichen Auswirkungen auf Einzelpersonen, Unternehmen und Regierungen. Viele nationale Vorschriften wurden erlassen, um sicherzustellen, dass alle grenzüberschreitend ausgetauschten Daten das gleiche Maß an Datenschutz, Sicherheit und Privatsphäre erhalten, wie die Daten innerhalb der Gerichtsbarkeit übertragen werden. Grundrechte und Grundwerte sollten laut Europäischer Union die Eckpfeiler des Datenschutzes sein. Die staatliche Datenkontrolle wird in der Volksrepublik China im Gegensatz zur Datenkontrolle des Privatsektors in den Vereinigten Staaten von Amerika priorisiert. Darüber hinaus haben mehrere Regierungen die Datenlokalisierung befürwortet, weil sie nicht verstanden haben, wie Daten auf globaler Ebene unter Einhaltung der geltenden Gesetze gehandhabt werden. Diese Thesis zielt darauf ab, zu untersuchen, ob Daten geteilt werden können, während sie innerhalb der Mitgliedsstaaten der Europäischen Union und international vollständig geschützt sind. Auf dem Weg zum Abschluss der Thesis wird ein Überblick über globale Trends und Einstellungen zum Datenaustausch und Datenschutz zwischen Ländern, Einzelpersonen und Unternehmen gegeben. Darüber hinaus wird die Komplexität der Datenlokalisierung im Vergleich zu den vielen Formen der Zusammenarbeit bei der gemeinsamen Nutzung von Daten, wie Open Data, bilateralen und plurilateralen Vereinbarungen sowie zahlreichen internationalen Vereinbarungen, die darauf abzielen, gemeinsame Standards zu etablieren, hervorgehoben.

Stichworte: Datenaustausch, Datenschutz, grenzüberschreitend, Privatsphäre, offene Daten, Einschränkung, Datenlokalisierung

TABLE OF ABBREVIATIONS

AI	Artificial Intelligence
AI Act	Artificial Intelligence Act
APEC	Asia Pacific Economic Cooperation
ASEAN	Association of Southeast Asian Nations
CCPA	California Consumer Act
CFR	Charter of Fundamental Rights of the European Union
CIIOs	Critical Information Infrastructure Operators
CJEU	Court of Justice of the EU
COPPA	Children's Online Privacy Protection Act
CPTPP	Comprehensive and Progressive Agreement for the Trans-Pacific Partnership
DEPA	Digital Economy Partnership Agreement
DMA	Digital Markets Act
DPA	Data Protection Authority
DPD	Data Protection Directive
DSA	Digital Services Act
DSL	Data Security Law
ECHR	European Convention of Human Rights
ECPA	Electronic Communications Privacy Act
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
e.g.	Exempli gratia
etc.	Et cetera
EU	European Union
FCRA	Fair Credit Reporting Act
FIPPs	Fair Information Practice Principles
FTA	Free Trade Agreements
FTC	Federal Trade Commission
GAPP	Generally Accepted Privacy Principles
GATS	General Agreements on Trade in Services
GDPR	EU's General Data Protection Regulation
GLBA	Gramm-Leach-Bliley Act

HIPAA	Health Insurance Portability and
HITEHA	Health Information Technology for Economic and Health Act
ICT	Information and Communication Technology
IDP	Industrial Data Platforms
IDTA	International Data Transfer Agreement
i.e.	id est
IoT	Internet of Things
ISO	International Organisation for Standardisation
MLAT	Mutual Legal Assistance Treaty
NIS Directive	EU Network and Information Security Directive
NIST	National Institute of Standards and Technology
NOYB	None of Your Business
OECD	Organisation for Economic Cooperation and Development
OGP	Open Government Partnership
PDP	Personal Data Platforms
PETs	Privacy-Enhancing Technology
PIPL	Personal Information Protection Law of the PRC
PRC	People's Republic of China
SCA	Stored Communications Act
SCCs	Standard Contract Clauses
TIA	Transfer Impact Assessment
UDPDA	Uniform Personal Data Protection Act
U.S. /United States	United States of America
USMCA	United States, Mexico, and Canada Agreement
VPPA	Video Privacy Protection Act
WP29	Article 29 Working Party
WTO	World Trade Organisation

INTRODUCTION

Data and data sharing are an indispensable part of progress, not only of the economy, digital economy and other business processes but also of innovations and digitalisation, which includes data-intensive technologies in the first place. However, the main issue regarding data sharing is that the increased need for different data types leads to higher risks for data and cyber security, data privacy, IPR protection and sovereignty. Countries do not have a unified approach to data protection, processing and collection. While some allow easy cross-border data sharing or open data flow, others have introduced additional laws, standards and policies to limit data transfer. The EU General Data Protection Regulation forms a complicated but powerful framework that provides comprehensive data protection. In addition, the European Union has been emphasising data re-use and sharing to enhance the European Union's digital market and improve its competitiveness in the global digital market. The main obstacle to achieving this goal are the data protection principles incorporated into the General Data Protection Regulation, which are not easy to reconcile with the idea of data sharing or open data flows. It is worth mentioning that other countries worldwide have also started to follow the General Data Protection Regulation model. In the United States, state laws aim to protect data privacy at the sectoral level, which does not restrict data movement outside the United States. The United States' approach, based on the accountability principle and its participation in the APEC Cross-Border Privacy Rules, has enabled it to be one of the leaders, in the global digital market. Other countries in the world are not able to apply their laws across borders, as the U.S. does, due to the lack of full cooperation between them. To overcome barriers and establish trust, there are also more policy frameworks allowing data sharing. Policy frameworks such as APEC's Cross-Border Privacy Rules would enable businesses to share data with specific recipients regularly. Many trade agreements and plurilateral and unilateral approaches have been established to overcome data sharing restrictions to protect privacy.

The reason for data localisation is that international data transfers of personal information cannot be effectively safeguarded, and the protection of individuals' rights abroad is insufficient. Therefore, adequate national protection of data privacy and a suitable system for cross-border data sharing would solve these barriers. The primary rationale for doing the aforementioned is that unrestricted cross-border data sharing benefits countries and their citizens as well as businesses.

I. CLARIFICATION AND CLASSIFICATION OF DATA

Data is a crucial element of the digital age, serving as the foundation for all commercial, government, and social activities that drive innovations and generate different benefits and competitiveness.[1] Data is a unique resource with distinct features. It is intangible and non-rivalrous, meaning data can be used and reused in various ways without being depleted.[2] In theory, (raw) data represents records of observations or actions, patterns of symbols designed and stored to be consistent with a particular purpose. However, data have no value until it is collected, sorted, verified, analysed, and processed into information and knowledge that can be utilised for commercial and societal reasons.[3] Nowadays, data is most commonly transferred or stored digitally, allowing for rapid allocation with positive and negative outcomes.[4] Global data movement, together with technical innovation, is also a crucial component in increasing data value. Therefore, data represents a diverse commodity whose value is determined based on context, with different impacts on individuals, businesses, and regulators.[5] Although data is the most valuable resource in the digital age, there is still a debate about defining and classifying data correctly.

Data classification based on different taxonomies is required to determine the national and international strategy and regulation needed for each data type, the manner in which the data is processed, and a policy to regulate cross-border data flows. Data classification is also necessary to understand data portability and determine how different actors participate in data formation.[6] The classification of data according to the manner in which it originated includes provided data, observed data, derived data, inferred data and acquired data.[7]

---

[1] Schwartz, P.M. and Solove, D.J. (2014) '*Reconciling Personal Information in the United States and European Union*', *California law review*, 102(4), pp. 877–916.,p.879, UC Berkeley Public Law Research Paper No. 2271442, GWU Legal Studies Research Paper No. 2013-77, GWU Law School Public Law Research Paper No. 2013-77, Available at SSRN: https://ssrn.com/abstract=2271442 [Accessed on 01 February 2022];

[2] UNCTAD (2021), *Digital Economy Report - Cross-border data flows and development: For whom the data flow*, United Nations Publications, p XVI, Available at: https://unctad.org/webflyer/digital-economy-report-2021; [Accessed on 13 February 2022];

[3]Ibid;

[4] Lowrance. (2012). *Privacy, Confidentiality, and Health Research* (Vol. 20). Cambridge University Press. p.7, https://doi.org/10.1017/CBO9781139107969, [Accessed on 01 February 2022];

[5] Casalini, F., J. López González and T. Nemoto (2021), "Mapping commonalities in regulatory approaches to cross-border data transfers," *OECD Trade Policy Papers*, No. 248, OECD Publishing, Paris, p.12, https://doi.org/10.1787/ca9f974e-en. [Accessed on 01 February 2022];

[6] OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, OECD Publishing, Paris,p.30. https://doi.org/10.1787/276aaca8-en. [Accessed on 01 February 2022];

[7] OECD (2014), Summary of OECD Expert Roundtable: "*Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*", OECD, Paris, p.5 Available at: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%282014%293&doclanguage=en; [Accessed on 01 February 2022];

- Provided/volunteered data come from direct, intentional actions taken by individuals. In this case, it must be intuitive or obvious that this data is created.[8] Provided data can be further divided into initiated, transactional, and posted data.[9] *Initiated data* is created by an action taken by an individual during which a connection is activated (e.g. registration for voting). *Transactional data* is generated when a person conducts transactions (e.g., paying a bill by credit card). *Posted data* is formed when individuals express themselves and are aware that they are doing so in a way that others will see or hear (e.g. sharing data on a social media platform).[10]

- Observed data represents data that others have observed and recorded in digital format, which can be recorded at the time of creation or after observation. The data controller plays an active role, whereas the data subject plays a passive one. The data subject may not be aware of data collection.[11] Face recognition and the Internet of Things (hereinafter "IoT") enables digital observation in the physical world. Given an individual's awareness levels, this type of data encompasses engaged, not anticipated, passive data. *Engaged data* includes data obtained from online cookies, loyalty cards, and other occurrences in which an individual is aware of observation at a particular time. *Not anticipated data* represent data that individuals did not know would be created. Namely, in this case, individuals are aware of the sensors but are not aware that these sensors create data. *Passive data* implies data created in a situation when it was very difficult for individuals to know that they were being observed and that data was being created.[12]

- Derived data are generated from other data and then turned into new data elements associated with a specific individual. Derived data is generally generated relatively mechanically, employing simple reasoning and basic mathematics to detect patterns and create classifications within a data set.[13] This data type is divided between *computational data*, representing data generated by applying an arithmetic method

[8] Ibid;
[9] Abrams, M. (2014), *The Origins of Personal Data and its Implications for Governance*, p.6. Available at SSRN: https://ssrn.com/abstract=2510927 [Accessed on 07 February 2022];
[10] The General Data Protection Regulation only applies to the provided/volunteered and observed data
[11] OECD (2014), Summary of OECD Expert Roundtable: "*Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*", (n 7);
[12] Abrams, M. (2014), *The Origins of Personal Data and its Implications for Governance*,(n.9),p.7;
[13] OECD (2014), Summary of OECD Expert Roundtable: "*Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*", (n 7);

to existing numerical features, and *nationally data*, characterised by new data elements established by categorising individuals as group members based on shared characteristics.[14]

- Inferred data is generated using probability-based analytical processes. They result from identifying intercorrelations, which are then used to create predictive behaviours, after which individuals are classified (e.g. statistics and advanced analytical data).[15] There are again two subgroups which include *statistical data,* which represents data based on statistical processes and where the individual is not involved in the creation of this data (e.g. credit risk assessment), and *advanced analytical data*, which is the result of analysing larger and complex data sets, and where the components are based on an evaluation that is more reliant on connection than causality.[16]
- Acquired/purchased/licensed data is data collected from other parties through commercial licensing agreements or another non-commercial way, in which contractual and other legal obligations may affect data re-use and sharing.[17]

From the standpoint of human rights protection and the economic value of data, the most significant classifications include personal or non-personal, private or public, and sensitive or non-sensitive data.[18]

Personal data differs from other data types due to its inseparable connection to the data source, i.e. individuals.[19] Personal data, personally identifiable information (hereinafter "PII") or personal information (hereinafter "PI") define the scope of privacy regulation and serves as

[14] Abrams, M. (2014), *The Origins of Personal Data and its Implications for Governance*,(n 9),p.8;
[15] OECD (2014), Summary of OECD Expert Roundtable: "*Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*",(n 7);
[16] Abrams, M. (2014), *The Origins of Personal Data and its Implications for Governance*,(n 9),p.8;
[17] OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*,(n.6)p.31;
[18] These classifications are not exclusive. Other possible classifications include structured and unstructured data, data for commercial purposes or governmental purposes; data used by companies, including corporate data, human resources data, technical data and merchant data; instant and historical data; and business-to-business (B2B), business-to-consumer (B2C), government-to-consumer (G2C) or consumer-to-consumer (C2C) data. *See* UNCTAD (2021), *Digital Economy Report - Cross-border data flows and development: For whom the data flow*, ,(n 2), p.7;
[19] Yakovleva, S. (2018) "*Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?,*" World Trade Review. Cambridge University Press, 17(3), pp. 477–508. p.481 Available at: https://doi.org/10.1017/S1474745617000453, [Accessed on 05 February 2022];

a judicial driver around the globe.[20] The progress of data processing techniques, which allows vast amounts of data to be moved across national boundaries, demands the creation of universal rules to protect individuals.[21] After data is classified as personal data[22], it is governed by applicable privacy legislation, which regulates the accessibility and sharing of such data. Additional agreements and regulations will likely govern personal data transfers across borders.

The approaches to governing personal data taken by the world's leading geopolitical and economic players differ significantly. This causes integration or interoperability issues between them, substantially impeding the ability to create comprehensive regulations to control data transfer across borders. The European Union (hereinafter "EU") approach prefers individual data control based on fundamental rights and values. The People's Republic of China (hereinafter "PRC") approach prioritises government data control, whereas the United States of America (hereinafter "U.S." or "United States") is centred on private-sector data control. Countries outside these data realms will probably have to choose which data governance approaches to embrace if differences continue to grow. The U.S., the PRC, and the EU seek to exert influence over other countries through trade agreements, developing and enhancing activities and resources required to survive and function effectively in a fast-evolving environment or strengthen their market dominance in return for market access. [23]

The legislative framework for data protection in the EU has acted as a model for data protection rules in numerous non-EU nations.[24] This is known as the *Brussels effect*. New privacy regimes in Brazil, Thailand, Panama, Barbados, and even the Personal Information Protection Law (hereinafter "PIPL") in the PRC, the California Consumer Act (hereinafter "CCPA")[25] in the U.S., and many other jurisdictions demonstrate the EU continued influence.

---

[20] van den Hoven, Jeroen, Martijn Blaauw, Wolter Pieters, and Martijn Warnier, Edward N. Zalta (ed.) (2020) "Privacy and Information Technology", *The Stanford Encyclopedia of Philosophy* , Available at: https://plato.stanford.edu/entries/it-privacy/; [Accessed on 10 February 2022];

[21] OECD (2002) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD Publishing. Available at: https://doi.org/10.1787/9789264196391-en.. [Accessed on 08 February 2022];

[22] Some countries use Personally Identifiable Information or Personal Information instead of personal data when referring to types of information that may identify a person. While personal data is used in the European Union, PII is used primarily in the United States and PI in CCPA, China and Canada. The PII and personal data are very similar, but not the same. All PII are personal data, but not all personal data are PII. The European Union has a uniquely broad definition of personal data, while the meaning of PII and PI is defined differently.

[23] UNCTAD (2021), *Digital Economy Report - Cross-border data flows and development: For whom the data flow*, (n 2),p. 116;

[24] Bradford, Anu. (2020) "*How the EU Became a Global Regulatory Power." In The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press. Oxford Scholarship Online, p.22. Available at: https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190088583.001.0001/oso-9780190088583-chapter-2; [Accessed on 08 February 2022];

[25] The California Consumer Act, A.B.375, 217 Gen Assemb., Reg. Sess. (Cal.2018);

Personal data is defined as follows in Article 4 (1) of the EU's General Data Protection Regulation (hereinafter "GDPR")[26]: *"any information relating to an identified or identifiable natural person ("data subject")".*[27] The GDPR refers to personal data processed entirely or partially by automated or non-automated means. The key components of personal data are "any information," "relating to," "identified or identifiable," and "natural person.":

- Any information - involves all kinds of information, subjective and objective, relating to a particular person, including even data that does not identify a specific person on its own but does so alongside other data, regardless of the format. The information must refer to a natural person and not to legal entities. The following information categories (sensitive and non-sensitive) can be used to identify individuals, such as:[28]
    1. Internal - information about knowledge and beliefs (e.g. religious beliefs[29], philosophical beliefs, thoughts, etc.), authenticating (e.g. passwords, PIN, etc.), preferences (e.g. opinions, intentions, interests, etc.) ;
    2. External – data which can be used to determine an individual's identity (e.g. name, picture, biometric data, user name, etc.), ethnicity (e.g. race, national or ethnic origin,[30] languages, etc.), sexual identity (e.g. gender identity, preferences, etc.), behavioural (e.g. on-line or off behaviour, browsing behaviour, links clicked, etc.) demographic (e.g. age ranges, income brackets, geographic, etc.), medical (e.g. family or individual health records[31], prescriptions, etc.), and information about a physical characteristic (e.g. height, weight, age, hair colour, gender, etc.);

---

[26] 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 2016 L 119/1;

[27] This concept of personal data is also defined in Article 2 (a) of the Convention no. 108 for the protection of individuals concerning the automatic processing of personal data and exemplified European Court of Human Rights in the Case of *Amann v. Switzerland* [GC], no. 27798/95, ECHR 2000-II, paragraph 65;

[28] CATEGORIES OF PERSONAL INFORMATION, IAPP, available at: https://iapp.org/media/pdf/resource_center/Categories-of-personal-information.pdf; [Accessed on 13 February 2022];

[29] See *Sinan Işık v. Turkey*, no. 21924/05, ECHR 2010, paragraph 37;

[30] See *S. and Marper v. the United Kingdom*, [GC], ECHR 2008, paragraph 66;

[31] In the case of *Z v. Finland*, the ECtHR stated that the protection of personal data, especially medical data, is critical to a person's right to privacy. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the ECHR and in maintaining trust in the health industry in general. As a result, domestic law must provide adequate measures to protect such interaction or disclosing personal health data as far as it is inconstant with the guarantees in Article 8 of the ECHR. The interest in preserving the confidentiality of these data will be primarily decided by determining whether the interference was proportionate to the legitimate goal pursued. Unless justified by a compelling public interest requirement, such interference is inconsistent with Article 8. of the ECHR. *See* Z v. Finland, ECHR 1997, Reports of Judgments and Decisions 1997-I, paragraphs 96,113 and 114;

3. Tracking – information about computer devices (e.g. e that an individual uses for personal use, IP address[32], etc.), location (e.g. information on the individual GPS location[33], country, room number, etc.), contact (e.g. email address, physical address, tel. number etc.);
4. Social - information about education or profession (e.g. salary, work history, school attended, employee files, etc.), criminal activity (e.g. convictions, charges, etc.), family (e.g. siblings, marriages, divorces, relationships, etc.), public life (e.g. general reputation, social status, political affiliations[34], interactions, communications meta-data, etc.), social network (e.g., friends, acquaintances, associations, etc.), communication (e.g. telephone recordings, voice mail, email, etc.);
5. Financial - information about an individual's financial account[35] (e.g. credit card number, bank account, etc.), ownerships (e.g. cars, houses, apartments, etc.), transactional (e.g. purchases and spending, income, loan records, taxes, etc.) credit standing, etc.;
6. Legal – e.g. information enclosed in a residence permit application and in legal analysis which contains information concerning an individual;[36]
7. Historical - information about an individual's personal history, etc.

- <u>*Relating to*</u> – Data "relates to" an individual when it refers to that person's identity, attributes, or behaviour, or when that information is used to decide or affect how that

[32] In the case of *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, the Court of Justice of the EU held that Internet users' static IP addresses were classified as personal data since they enable users to be precisely identified. *See* C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), EU:C:2011:771, paragraph 51;

[33] In the case of *Uzun v. Germany*, the ECtHR ruled that data collected by a GPS is personal data that can disclose an individual's location and public movements. The processing and use of the data collected in this manner interfered with his right to respect his private life under Article 8(1) of the European Convention of the Human Rights (formally „*Convention for the Protection of Human Rights and Fundamental Freedoms*"), *See* Uzun v. Germany, no. 35623/05, ECHR 2010, paragraphs 51-52;

[34] In the case of *Catt v. the United Kingdom*, the ECtHR personal data disclosing political opinions is one of the particular types of sensitive data that requires additional protection measures. Moreover, the ECtHR stated that it is unjustified for national authorities to ignore this aspect by processing such data in compliance with domestic regulations without considering the requirement for additional protection. See *Catt v. the United Kingdom*, no. 43514/15, ECHR 2019, the ECtHR, paragraph 112;

[35] Information obtained from an individual's banking documents constitutes personal data, which is ruled by the ECtHR that considered the issue of financial data collection, processing, and disclosure associated with financial data transfer to authorities in another country that is not a signatory to the Convention in the case of *G.S.B. v. Switzerland*, no. 28601/11, ECHR 2015, paragraph 50;

[36] Legal analysis which contains only an abstract legal interpretation does not qualify as a personal data; *See* Joined Cases C-141/12 and C-372/12 YS [2014] EU: C:2014:2081, *YS v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v M and S*, paragraph 47;

person is regarded or assessed.[37] This element is essential in shaping the concept's context, especially concerning objects and technological innovations. The interpretation suggests three alternative components to determine whether information "relates to" an individual: content, purpose, or result. The *"content"* component is visible in cases when information is given to a specific individual, regardless of the purpose of the data controller or a third party or the repercussions on the data subject. If information "relates" to a person, it must be "about" that person, which needs to be evaluated by considering the circumstances of the particular case. That *"purpose"* element exists if the data are used or are expected to be used to assess, treat, or influence an individual's state or behaviour. Even if the *"result"* component is the only one that exists, data might be regarded as "related" to an individual since their usage will impact that individual's rights and interests. In this case, it is sufficient that the individual may be treated differently from other people due to such data processing.[38]

- An identified or identifiable –The identified natural person is a person who can be distinguished from all other natural persons. An identifiable natural person[39] is a person that can be identified, even though they still have not been. Identification is accomplished through unique pieces of information known as "identifiers" that have a close connection with the particular individual.[40] The GDPR contains a list of standard identifiers that may help individuals to which the data relates to being identified.[41] The concept of "direct"[42] or "indirect"[43] identification implies that the scope, to which particular identifiers are suitable for identifying a person, is context-dependent. The person's name is the most obvious identifier for "directly" identified or identifiable persons. The term "indirectly" identified or identifiable persons are typically associated with "unique combinations". When the scope of available identifiers does not identify a specific individual, that individual may be "identified"

[37] Article 29 Working Party (2005), "Working document on data protection issues related to RFID technology", WP 105, p.8. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf; [Accessed on 15 February 2022];
[38] Article 29 Working Party (2010), *Opinion 04/2007 on the Concept of Personal Data*,(WP 136) 01248/07/EN, p.10. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf; [Accessed on 15 February 2022];
[39] See case of *Benedik v. Slovenia*, no. 62357/14, ECHR 2018, paragraph 111;
[40] Article 29 Working Party (2010), *Opinion 04/2007 on the Concept of Personal Data*,(n 38), p.12;
[41] Article 4 (1) of the GDPR;
[42] See *Guillot v. France,* no. 22500/93, ECHR 1996, paragraphs 21-22;
[43] Case of *Benedik v. Slovenia*, (n.39), paragraphs 107-109;

since the individual may be distinguished from everyone else when paired with other pieces of information.

- Natural person - The right to protect personal data applies to a natural person. This refers to Article 6 of the Universal Declaration of Human Rights,[44] which states, "*Everyone has the right to recognition everywhere as a person before the law*".[45] In this context, the right to personal data protection is universal and not restricted to residents and citizens of a single country. The Recital 27 specifies that the GDPR only applies to living individuals and does not apply to the deceased or legal persons[46]. However, in certain ways, deceased individuals may be indirectly protected, mainly if that personal data includes information about people who are still alive. Moreover, it is not clarified what living individuals mean and whether or not it includes unborn children. Even though personal data protection appears to be primarily associated with individuals in terms of their right to respect for their private life under Article 8. of the European Convention of Human Rights (hereinafter "ECHR"), legal entities may also invoke this right before the European Court of Human Rights (hereinafter "ECtHR") if they are affected by a measure that violates their right to respect for their "home" or "correspondence".[47]

The term "*personally identifiable information*" is used in the United States. This term covers both identified and identifying data, eliminating all distinctions between "identified" and "identifiable.". Numerous regulations in the U.S. acknowledge this term and term PI (e.g.CCPA).[48] The legal system in the United States comprises federal and state laws and sector-specific regulations, and they all define and categorise various types of information as PII or PI. Personal information is determined by the CCPA as "*information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.*" [49] This concept is a broad legal interpretation of what represents personal information, noting that it contains any data

[44] UN General Assembly. (1948). *Universal declaration of human rights* (217 [III] A). Paris;
[45] Ibid, p.21;
[46] Recital 14 of the GDPR;
[47] See *Bernh Larsen Holding AS and Others v. Norway*, no. 24117/08, ECHR 2013, paragraph 106;
[48] Schwartz, P.M. and Solove, D.J. (2014) 'Reconciling Personal Information in the United States and European Union', (n 1), p. 887;
[49] CCPA, Article 1798.140 (v)(1);

that can be linked to a California consumer or household.[50] This extends beyond data associated with a direct individual's identification, such as a person's name, birth date, or social security number, which has historically been PII. Indirect information (e.g. geolocation data) is crucial because it is much harder to identify and link to a data subject. This definition of the PI is substantially similar to the meaning of personal data under the GDPR. However, the main difference between these two regulations is that the CCPA definition also includes information linked to the household, while the GDPR does not. The moment where the information has become identifiable enough to fall under a specific jurisdiction is defined according to how each information privacy statute defines its specialised concept of personal information.[51] Additionally, not only is the term used differently, but the meaning of personal data and PII concepts appear to be contradictory in the U.S. and EU regulatory frameworks. There are three main approaches to defining PII in the United States such as the "tautological", the "non-public", and the "specific type" approach.[52]

1) *The tautological approach* represents a standard in which PII is described, like any information that could identify a person, such as the interpretation displayed in the Video Privacy Protection Act (hereinafter „VPPA“)[53]. The advantage of this approach is being accessible by nature rather than closed and it is adaptable to new trends. A problem with the tautological approach is that it does not explain PII or specify how it should be recognised.
2) *The non-public approach* defines PII by emphasising what it isn't, instead of what it is. The concept of publicly available information and purely statistical data underpins the non-public approach. This model would exempt the information in these two categories from PII. The Gramm-Leach-Bliley Act (hereinafter „GLBA“) exemplifies this approach by specifying personally identifiable financial information as "nonpublic personal information".[54] Not determining whether or not the information is identifiable

[50] The CCPA defines "*consumer*" as a California resident for tax purposes. Because a California resident is a living person, information about deceased people, unborn children or legal entities are not regarded as PI. CCPA does not define "household.";
[51] Schwartz, P.M. and Solove, D.J. (2014) '*Reconciling Personal Information in the United States and European Union'*, (n 1), p.888;
[52] Schwartz, P.M. and Solove, D.J. (2011) 'The PII Problem: Privacy and a new concept of personally identifiable information, *New York University law review (1950)*, 86(6), pp. 1814–1894.,p.1829;
[53] Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (a)(3);
[54] Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6809(4)(A);

is the main disadvantage of this approach. The status of data, as public or private, does not always relate to whether or not it should be used to identify the person.[55]

3) *The specific-type approach* identifies particular categories of information that fall under the scope of personal information. The Children's Online Privacy Protection Act (hereinafter „COPPA“)[56] illustrate a specific-type approach and stipulates that personal information includes individually identifiable information, about an individual, gathered digitally, such as first and last names, social security numbers, phone numbers, email addresses, as well as other identifiers that the Federal Trade Commission (hereinafter "FTC") designates as allowing physical or online contact with a specific individual[57]. In 2000, through the COPPA Rule[58], the FTC added persistent identifiers linked to personally identifiable information to this list, such as a consumer number stored in a cookie or a processor serial number.[59] Although this approach is quite constrained, it is more concise than the other two. Nevertheless, it does not provide a concept or method for determining whether a type of information should be included or excluded from the list.[60]

All three methods are insufficient and do not offer clear guidelines for what type of information constitutes the PII.

Non-personal data has emerged as the most recent subject to be considered. Non-personal data may freely flow in the digital environment and is the most popular choice for global data exchange. It is viewed as a source of domination for technological businesses that exploit data and insights for business purposes. Sharing this data may help balance power in the data economy.[61] Completely contrary, for the flow of personal data, specific requirements need to be fulfilled (e.g., consent, risk assessment, etc.).[62] Non-personal data include data that

[55] Schwartz, P.M. and Solove, D.J. (2011) "The PII Problem: Privacy and a new concept of personally identifiable information", (n 52), p. 1830;
[56] Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 – 6506;
[57] Ibid., §§ 6501 (8)(A)-(G);
[58] 16 CFR. § 312.2;
[59]Schwartz, P.M. and Solove, D.J. (2011) "The PII Problem: Privacy and a new concept of personally identifiable information", (n 52), p. 1832;
[60] Ibid.,p.1835;
[61] Kapoor, A., and Amrita N. "*Non-Personal Data Sharing: Potential, Pathways and Problems*." CSI Transactions on ICT, vol. 9, no. 3, Springer India, 2021, pp. 165–169, p.165. Available at: https://doi.org/10.1007/s40012-021-00336-5; [Accessed on 11 February 2022];
[62] Podda, E. and Palmirani, M. (2021) 'Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data', in *AI Approaches to the Complexity of Legal Systems XI-XII*. Cham: Springer International Publishing, pp. 269–282. p. 270; Available at: https://link.springer.com/chapter/10.1007/978-3-030-89811-3_19; [Accessed on 08 February 2022];

is always non-personal because it will never be linked to an identified or identifiable natural person, and data that was once personal but is no longer so because the link to a natural person has been eliminated.[63] As stated in article 3. of the Free Flow of Non-personal Data Regulation**,** non-personal data represents data other than personal data as defined in Article 4 (1) of Regulation (EU) 2016/679[64]. Therefore, according to this Regulation, the definition of non-personal data is entirely reliant on the meaning of personal data.

Furthermore, to differentiate between personal and non-personal data, Recital 26. of the GDPR does include a legal test that essentially employs a risk-based approach. According to this legal test, data should be considered personal when there is a reasonable risk of identification. Whenever the risk is purely negligible, the data may be regarded as non-personal, even if identification cannot be precluded entirely. However, several aspects of this test are ambiguous due to the different perceptions of different authority supervisors.[65] Uncertainties exist over if it is necessary to concentrate solely on the data controller (a relative/subjective approach) or any third party (an absolute/objective approach)[66], to determine whether a reasonable risk of identification exists.[67] The United Kingdom employs a third approach to conducting this type of test, known as "*motivated intruder*". The "motivated intruder" is someone who begins with no previous knowledge but wants to identify the individual whose personal data was used to generate the anonymised data. The approach presumes that the "motivated intruder" is reasonably competent and has access to different resources and investigative techniques.[68]

---

[63] Finck, M. and Pallas, F. (2020) '*They who must not be identified—distinguishing personal from non-personal data under the GDPR*', International data privacy law, 10(1), pp. 11–36. doi:10.1093/idpl/ipz026. p.13; [Accessed on 19 February 2022];

[64] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union;

[65] Recital 26 of the GDPR, *see* Finck, M. and Pallas, F. (2020) '*They who must not be identified—distinguishing personal from non-personal data under the GDPR*', (n 63);

[66]In case of *Patrick Breyer v Bundesrepublik Deutschland,* the CJEU confirms the risk-based approach noted in GDPR Recital 26. The court concluded that dynamic IP addresses could be considered "personal data," despite the fact that only a third party (in this case, an internet service provider) had the extra information required to identify the individual under specific circumstances. The ability to link the data with this extra data must be "reasonably likely to be used to identify" the individual. The so-called "absolute/objective approach," which believes that material is already "personal data" if any third party (globally) can identify the individual's identity, has not been employed. Dynamic IP addresses shall not be deemed personal data where the linking of the IP address with other data permitting identification is prohibited by law, or when that data can only be obtained by disproportionate measures in terms of time, expense, or human resources. See C-582/14: *Patrick Breyer v Bundesrepublik Deutschland,* ECLI:EU:C:2016:779, (paragraph 46);

[67] Finck, M. and Pallas, F. (2020) '*They who must not be identified—distinguishing personal from non-personal data under the GDPR*',(n 63),p.17;

[68] Information Commissioner's Office (2012), '*Anonymisation: Managing Data Protection Risk Code of Practice*', p.22. Available at: https://ico.org.uk/media/1061/anonymisation-code.pdf; [Accessed on 03 March 2022];

As for the U.S. strategy, non-PII is known as information that cannot be used to trace or identify an individual's identity. Device IDs, cookies, and IP addresses are not considered PII in the majority of the United States. However, some states, such as California[69] and New Jersey[70], classify this data as PI or PII. Several pieces of legislation considers the addition of data categories to the list of PII (e.g. COPPA, the False Identification Crime Control Act [71]). Besides the explicit recognition that an IP address could be personally identifiable and qualifies as data worth protecting, no changes are required for these and related statutes.[72] In addition, the distinction between PII and non-PII is constantly changing in response to context and evolving technology.[73] According to the CCPA, information available to the public is not recognised as PI. "*Publicly available*" refers to legally available information from federal, state, or local government documents, subject to any conditions. "Publicly available" does not correspond to biometric data collected about a consumer without his knowledge, as well as deidentified or aggregated consumer data. Information is also not "publicly available" if used for a reason incompatible with the purpose for which it is preserved and made accessible in government records or publicly maintained. The CCPA, does not classify or exclude pseudonymous data as PI.

The PIPL[74], like the GDPR, considers anonymised information to be non-personal information and thus outside of the scope of the law.[75] The concept of anonymisation is stringent and represents the process that transforms personal information so that it cannot be used to identify a specific natural person and cannot be reversed.[76]

---

[69] The CCPA provides a list of examples of personal information which explicitly includes IP addresses, but only if the identifier "*identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household*."(CCPA § 1798.140(o)(1));
[70] In the case of *State v. Reid*, the New Jersey Supreme Court held that Because Internet subscriber information is considered confidential, it is protected from disclosure. While it may not have infringed privacy rights under the U.S. Constitution, the New Jersey Supreme Court ruled that the New Jersey Constitution provides expanded privacy rights that were violated. Article I, Paragraph 7 of the New Jersey Constitution protects an individual's privacy interest in subscriber information given to an Internet service provider. At the same time, the federal constitution does not explicitly guarantee such a privacy right. See *State v. Reid, 945 A.2d 26 (2008),194 N.J. 386;*
[71] 18 U.S.C. § 1028(d)(7)(C) (2006);
[72] McIntyre, J.J. (2011) „*Balancing expectations of online privacy: why Internet Protocol addresses should be protected as personally identifiable information*", *The De Paul law review*, 60(3), p. 895. Available at: https://via.library.depaul.edu/cgi/viewcontent.cgi?article=1151&context=law-review; [Accessed on 06 March 2022];
[73] The U.S. Court of Appeals for the First Circuit issued an opinion in the case of *Yershov v. Gannett Satellite Information Network*, broadening the scope of the VPPA by endorsing a significantly expanded view of how the VPPA applies. In its decision, the court held that PII includes a device's GPS coordinates and a mobile app user. Also, those who do not pay or instead register to use the app qualifies as "consumer" entitled to the VPPA safeguards. See *Yershov v. Gannett Satellite Information Network, Inc., No. 15-1719*;
[74] Personal Information Protection Law of the People's Republic of China, No. 91(2021);
[75] Article 9. of the PIPL;
[76] Article 73(IV) of the PIPL;

Sensitive data is a crucial component of contemporary data protection. Its significance in data protection legislation was not always apparent, and debates about how to define it continue to this day. The nature and use of sensitive data have evolved quickly in recent years. With increasing computing dominance and the easiness of sharing and merging different data types, so much more data unquestionable will become sensitive. The quantity relies on the concept of sensitive data have been using. The scope of sensitive data, in particular, can differ based on whether a context-based or purpose-based definition is used. According to the *context-based approach*, any personal information can be sensitive based on the processing circumstances. The elements that could assist in determining the sensitivity of personal data processing include the controller's specific interests and the potential data users, the purposes for which the data are collected, the requirements of the processing, and the possible repercussions for the individuals concerned. A *purpose-based approach* examines the data controller's intention and if the controller intends to reach conclusions from specific data processing that could be considered sensitive. Overall, these intentions determine if the data used is sensitive or not. Therefore, this concept leads to the conclusion that no sensitive data is engaged when the controller has no interest in creating or using data in a manner that can be recognised as sensitive.

The need to eradicate forms of discrimination or their effects is typically linked to sensitive data. The requirement to preserve fundamental rights, i.e. protecting privacy, is the rationale for regulating sensitive data through strict legal frameworks.

The Organisation for Economic Cooperation and Development (hereinafter „OECD“) first proposed the concept of sensitive data on the international level in its Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (hereinafter "OECD guidelines")[77]. These non-binding guidelines indicate that OECD members need to incorporate the concept of sensitive data into national legislation. According to the guidelines, it is impossible to identify a set of data generally acknowledged as sensitive.[78]

In 1981, the Council of Europe adopted the Convention for the protection of individuals concerning the automatic processing of personal data (hereinafter "Convention No.108"*)*[79]. It was regarded as binding on signatories, although it did not require direct

[77] OECD (1980), *Guidelines on the protection of privacy and transborder flows of personal data*. Paris: OECD, Available at: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; [Accessed on 06 March 2022];
[78] Ibid, paragraph 19(a);
[79] Council of Europe (1981), *Convention for the protection of individuals with regard to automatic processing of personal data ,* (ETS 108);

incorporation into domestic legislation. Convention No.108 defined which data types should be considered sensitive, including personal information such as racial origin, political opinions or religious or other beliefs, health, or sexual life.[80] Signatories could generate different categories of sensitive data in national legislation. According to this Convention No.108, data sensitivity varies depending on the legal and sociological context of the country in question. The United Nations, for example, released the Guidelines for the Regulation of Computerised Personal Data Files (hereinafter "UN guidelines")[81] in 1990, rationalising additional safeguards for sensitive data since such data are likely to contribute to unjustifiable discriminatory practices. Compered to Convention No.108, the UN guidelines are broader since they encompass the categories of ethnic origin and colour while including membership in trade unions or other groups. However, they exclude criminal convictions and health information. Countries had the choice of employing an internationally accepted regulatory method to address risks connected with the processing of personal data under both Convention No.108 and the UN guidelines. They were allowed to create regulations that better aligned with their requirements.[82]

The Data Protection Directive (hereinafter "DPD")[83] states seven special categories of data that require additional protective measures, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sexual life.[84] The DPD stipulated extensive restrictions on those who wished to process sensitive data. This has been accomplished primarily by developing the appropriate legal bases that apply if sensitive data is processed. Overall, such legal bases were far more stringent and limited in scope than those applicable to those wishing to process non-sensitive data. The DPD differs from the Convention No.108 approach because it includes trade union membership as a special category of sensitive data, and the list of sensitive data is considered exhaustive. However, the DPD does not have a category of data on skin colour or membership in an association such as the UN Guidelines but does include the category of criminal convictions.

---

[80] Ibid, Article 6;
[81] UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990, available at: https://www.refworld.org/docid/3ddcafaac.html [accessed 15 January 2022]
[82] McCullagh, K. (2017), *Data Sensitivity: Proposals for Resolving the Conundrum. Journal of International Commercial Law and Technology*, Vol. 2, Issue 4, pp. 190-201, p. 2 Available at SSRN: https://ssrn.com/abstract=1378121[Accessed on 07 February 2022];
[83] 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, OJ 1995 L 281/31;
[84] Ibid, Article 8(1);

Special categories of personal data are given extra protection under the GDPR because their processing poses a severe risk to fundamental rights and freedoms.[85] The GDPR clarified and expanded the scope of protection by adding three new special categories of personal data, including genetic data, biometric data and data regarding sexual orientation.[86] Member States can no longer introduce additional types of sensitive data, as they could under the DPD. When transferring sensitive personal data, the data importer must implement other security measures applicable to the particular risk involved to restrict who has access to personal data. The ECtHR has used case law relating to Article 8. of the ECHR to guarantee that individual privacy is treated with respect in various circumstances.[87] This includes, most importantly, the obligation to protect personal data, particularly sensitive data. Except for personal data about criminal convictions, which is classified as one sequence of sensitive personal data along with the others and is governed by a separate article under the GDPR, the sub-categories of sensitive personal data under Turkey's Personal Data Protection Law[88] are also equivalent to the special categories of personal data under the GDPR.

The GDPR's special categories of data are recognised under Bosnia and Herzegovina's Law on Personal Data Protection (hereinafter „LPDP“)[89], which also emphasises that their processing is, in principle, prohibited.[90] Consent to process special category personal data must be expressed in precise and clear language, signed by the data subject, and explicitly specify the personal data for which it was provided, the controller, the processing purposes, and the period for which it was granted. All components of the data filing system request must be evaluated using a proportionality test and approved by the Personal Data Protection Agency.[91]

Similar to the description of the special categories of data under the GDPR, the PIPL in the PRC provides a definition of "sensitive data". Additionally, the PIPL definition, takes a step further, categorising sensitive data as any information that, if published or misused, might result in substantial harm to an individual.

---

[85] Recital 51. and Recital 71. of the GDPR;
[86] Article 9 (1) of the GDPR;
[87] The ECtHR in the case of *Gaughran v. the United Kingdom* states that in evaluating whether there has been an interference with a person's private life, it must consider the specific circumstances, for example under which the information in question was recorded and stored, the nature of the records, how these records are used and processed, and the results that may be generated. See *Gaughran v. the United Kingdom*, no. 45245/15, 13 ECHR 2020, paragraph 70;
[88] Turkey’s Personal Data Protection Law No. 6698 (2016), (Kişisel Verileri Koruma Kanunu - „KVKK“);
[89] The Law on Personal Data Protection (Official Gazette of BIH', nos. 49/06, 76/11, and 89/11, or Zakon o zastiti licnih podataka ("Sl. glasnik BiH", broj 49/06, 76/11, i 89/11));
[90] Article 3(a) of the LPDP;
[91] Article 5 of the LPDP;

Although, special/sensitive categories of personal information are not covered under the CCPA, it states that personal data includes, but is not limited to, biometric information, professional or employment-related information, education information, geolocation data, internet activity like browsing history or search history and identifiers like name, alias, and postal address, among others.[92] In the U.S., the California Privacy Rights Act (hereinafter „CPRA"), which will come into effect on January 1, 2023, defines a new type of personal information known as sensitive personal information. This new list comprises biometric data, race, ethnicity, sexual orientation, religious beliefs, geolocation, and social security numbers.

1. DEGREES OF DATA IDENTIFIABILITY

Data identifiability refers to the ability to identify a particular person within a dataset. In order to accomplish this, identifiers are used. Identifiers are pieces of information that distinguish a person from other natural persons. The range of identifiability varies from directly identified to indirectly identifiable to non-identifiable. Context is one of the essential factors in determining whether a specific data is valued as an identifier. In contrast, the sensitivity of the data, legal requirements and the risk of identifying individuals, are the key factors that necessitate the removal of identifiers.[93] Several de-identification and anonymisation techniques have been effective under U.S. and EU privacy laws. Data de-identification is a set of strategies and techniques used to remove identifiers from data. However, de-identified data can be re-identified or re-linked to individuals with the help of additional data sources.[94] Data anonymisation is a subset of de-identification that entails removing unique identifiers and putting security measures to prevent data from being re-identified. There is also pseudonymisation, which is a modification where personally identifying information is handled with pseudonyms or artificial identifiers held separately and subject to technical safeguards. Pseudonymisation regularly provides pseudonyms to be overturned, allowing data subjects to be identified again. For example, the Health Insurance

[92] CCPA, Section 1798.140 (o)(1);
[93] Lowrance, W. W. (2012) "Identifiability and person-specific data," in Privacy, Confidentiality, and Health Research. Cambridge: Cambridge University Press (Cambridge Bioethics and Law), pp. 87–110. p.94 Available at: https://doi.org/10.1017/CBO9781139107969.008; [Accessed on 04 March 2022];
[94] Achatz, C. and Hubbard, S. (2017) '*US vs. EU guidelines for de-identification, anonymization, and pseudonymization*', *Journal of Internet Law*, 20(11):1-10., p. 7.. Available at: https://uaccess.univie.ac.at/login?url=https://www.proquest.com/trade-journals/us-vs-eu-guidelines-de-identification/docview/1899442429/se-2?accountid=14682; [Accessed on 04 March 2022];

Portability and Accountability Act (hereinafter "HIPAA")[95] rules define only that a covered entity may reverse direct identifiers back to subject identities.

The ISO/IEC 19441 standard has been helpful for data access and sharing because it shows how data can be linked back to identity. This standard also aids in determining the level of privacy risk, which helps determine the necessary legal and technical safeguards. In theory, data which has been successfully anonymised and aggregated will be shared more openly because it is less likely to result in privacy violations. [96] These terms, as stated by the OECD[97], and guided by standard ISO / IEC 19441, are arranged in a hierarchy based on the risk of re-identification, as shown below: [98]

- *Identified data*: Data that can be linked to a specific person because it consists of direct or indirect personal identifiers. Identified data has the highest level of risk or absolute risk of re-identification;
- *Pseudonymised data*: Data containing pseudonyms and artificial identifiers that have replaced all identifiers are subject to technical safeguards and can be overturned by anyone other than the party who performed them. The risk of re-identification is negligible with this type of data.
- *Unlinked pseudonymised data*: This is the type of data where all identifiers are excluded or replaced by aliases, and the assessment function is deleted or irreversible. No reasonable effort can be made to re-establish the connection.
- *Anonymised data*: Unlinked data whose attributes have been altered so that the data, alone or in conjunction with other data, cannot be used to directly or indirectly identify a person. This data has been safeguarded by technical means so that it can never be re-identified. Therefore, there is no risk of re-identification.[99]
- *Aggregated data*: Statistical data that excludes personal records and is derived from information about numerous people make personal attributes unidentifiable.

According to the Recital 26 of the GDPR anonymous information is information that does not link to an identified or identifiable natural person.[100] A definition of pseudonymisation is present in the GDPR and Recital 26. The GDPR defines pseudonymous data as data in which

[95] The Health Insurance Portability and Accountability Act of 1996; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996;
[96] OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies* (n 6), p.27;
[97] Ibid;
[98] Ibid;
[99] Achatz, C. and Hubbard, S. (2017) '*US vs. EU guidelines for de-identification, anonymization, and pseudonymization*', (n 94), p8;
[100] Recital 26. of the GDPR;

the iden,tifiers in a dataset are replaced by artificial identifiers, or pseudonyms, that are stored separately and protected through technological mechanisms[101]. Although the European Data Protection Board (hereinafter "EDPB") does not support the Opinion of the Article 29 Working Party (hereinafter "WP29")[102], it is the only one in the EU to provide various guidelines and techniques related to implementing anonymisation and pseudonymisation. According to the Opinion of the Article 29 WP, anonymisation represent a technique applied to personal data to obtain irreversible deidentification[103]. The solution to eliminating the risk of re-identification is reflected in using the most likely and reasonable anonymisation techniques, such as randomisation and generalisation.[104] Randomisation is a technique that changes data validity to break the strong link between data and individuals. Because every record is generated from an individual, randomisation will not decrease the distinctiveness of each record. Still, it may protect against inference risk when used alone or in conjunction with other techniques. The additional methods can include noise addition, permutation/substitution and differential privacy.[105] At the same time, generalisation entails generalising the attributes of the subjects by changing the scale or order of magnitude. However, generalisation can effectively eliminate singling out while ineffective in preventing linkability and inference. Subcategories of the generalisation are L-diversity, aggregation and K-anonymity. The WP29 defines pseudonymisation as the process of changing personal identifiers with another. As a result, the individual can still likely be recognised indirectly.[106] Pseudonymisation, with its subcategories such as encryption and hashing, are insufficient to render data anonymous.

However, the EDPB did not endorse this Opinion 05/2014 of the WP29.[107] The EU has not taken an official opinion on anonymisation or pseudonymisation techniques. However, the Spanish Data Protection Authority ruled that hashing may be regarded as an anonymisation technique after performing a detailed risk assessment for reidentification.[108]

---

[101] Article 5. of the GDPR;
[102] Article 29 Working Party, Opinion 05/2014 on Anonymization Techniques, 0829/14/EN WP216, http://ec.europa.eu/justice/data-protection/ article-29/documentation/opinion-recommendation/files/2014/ wp216_en.pdf. [Accessed on 11 January 2022];
[103] Ibid, p.7;
[104] Ibid;
[105] Ibid, p.12;
[106] Ibid 20;
[107] EDPB (2018), *The European Data Protection Board Endorsement 1/2018,* Available at: https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf [Accessed on 11 January 2022]
[108] AEPD (2019), Introduction to the hash function as a personal data pseudonymisation technique,p.23. Available at https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf; [Accessed on 11 January 2022]

Deidentification, aggregation, and pseudonymisation are defined under the CCPA. Deidentification differs from GDPR's equivalent anonymisation definition because it requires policy/contractual conditions to be achieved. Under HIPAA, the Expert Determination Method and the Safe Harbor Method can deidentify private health information (PHI). An expert evaluates data and chooses a suitable method to de-identify the data with a low chance of reidentification. The National Institute of Standards and Technology (NIST) has released Personal Data Confidentiality Guidelines (hereinafter "the NIST Guidelines"), which offer many instructions and de-identification techniques for federal agencies that can also be used voluntarily by non-governmental organisations (NGOs). [109]

According to the NIST Guidelines, five techniques are used for de-identifying quasi-identifiers:[110]

- *Suppression*: Personal identifiers are suppressed or removed entirely in favour of random values. This can lead to increased privacy protection while decreasing the dataset's utility.
- *Generalisation*: Specific direct or indirect personal identifiers can be assigned to a range or a set member. The entire dataset and individual records can be generalised.
- *Perturbation:* Within a defined level of generalisation, personal identifiers can be replaced with other information consistently for each individual.
- *Swapping*: Within certain levels of generalisation, personal identifiers can be exchanged between records.
- *Sub-sampling:* The de-identification organisation can release a sample rather than distributing the entire dataset. The likelihood of reidentification decreases when only a subsample is released.

The PIPL defines de-identification as processing personal data so that specific persons cannot be identified without using supplementary data. Anonymisation is altering personal data so that it can no longer be used to identify particular persons and cannot be retrieved[111]. As a result, the PIPL follows the GDPR's strict anonymisation standards to a great extent.

Moreover, the anonymisation technique that can prevent sensitive data from being leaked and assure the validity of publicly available information is presented in the non-binding

[109] Ibid, p.9;
[110] NIST (2015), *Privacy Risk Management for Federal Information Systems, National Institute of Standards and Technology Internal Report 8053*, Washington, DC,p. 20. Available at http://dx.doi.org/10.6028/NIST.IR.8053; [Accessed on 08 January 2022];
[111] Article 73. of the PIPL;

White Paper on Big Data Security published by the Institute of Information and Communications Technology in 2018.[112]

In some other countries, such as Switzerland, there are no provisions defining anonymisation and pseudonymisation of data, nor have anonymisation or pseudonymisation techniques have been addressed, while in Ukraine, there is only one provision related to depersonalisation of personal data, which represents the removal of information that allows the direct or indirect identification of a person. [113]

2. PRIVATE-SECTOR AND PUBLIC-SECTOR DATA

Public sector data represents data collected by public bodies necessary to provide public services, monitor trends, and understand the needs of the population (e.g. statistics, administrative, geospatial data). Sharing this type of data increases efficiency in the public and private sectors, contributing to economic development and societal progress. Enhanced data access and sharing in the public and private sectors can, in general, result in positive social and economic benefits for data holders, their suppliers, and data users, as well as for the broader economy, through increased transparency, accountability, and user engagement, new business opportunities, competition and cooperation within and across sectors and countries, innovation, and enhanced data security.[114]

While there are numerous advantages to sharing public data, there are concerns associated with its misuse and security, such as inadequate quality and data management, competence, and societal perceptions. It is critical that data sharing, whether in the public or private sector, is done with particular respect for individuals' right to privacy.[115] The right to privacy is connected to individual control over data and the application of a legal basis for data processing (in most cases, it is consent). To mitigate the risks related to data sharing, privacy-

[112] Available at: https://digichina.stanford.edu/work/translation-big-data-security-white-paper-2018/; [Accessed on 12 February 2022];
[113] Article 2. of the Law"On Protection of Personal Data" of Ukraine, Official Bulletin of the Verkhovna Rada of Ukraine (BVR), 2010, No. 34, Art. 481. Available at:https://zakon.rada.gov.ua/laws/show/2297-17; [Accessed on 26 March 2022];
[114] OECD (2002), *Mapping approaches to data and data flows - Report for the G20 Digital Economy Task Force*. Paris: OECD Publishing, p.10 Available at: https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf; [Accessed on 12 February 2022];
[115] Pagliari, C., Davidson, S., Cunningham-Burley, S., Laurie, G., Aitken, M., Sethi, N. (2013). *Public Acceptability of Data Sharing Between the Public, Private and Third Sectors for Research Purposes.* Scottish Government Social Research, p.7, Available at: https://www.researchgate.net/publication/257963356_Public_Acceptability_of_Data_Sharing_Between_the_Public_Private_and_Third_Sectors_for_Research_Purposes; [Accessed on 12 January 2022];

enhancing technology (hereinafter "PETs", e.g. encryption techniques) or artificial intelligence (hereinafter "AI") can be utilised. A draft EU Data Governance Act was created to enhance data available for sharing between EU nations. At the same time, the G7 Trade Ministers agreed on Digital Trade Principles[116] to find a uniform legislative framework and foster interoperability, intending to free and dependable cross-border data flow.

The significant distinction between the private and public sectors is the foundation for processing personal data in terms of data sharing. Regulations are in place to control data processing in the public sector, and public agencies that carry out this type of processing must have a legal basis. Data is processed for socioeconomic reasons rather than personal gain in the public sector.[117]

While data processing in the private sector is contractual, the individual's consent is required, as is tight control. Personal interest is addressed in this instance. Furthermore, data processing is confined to a few public institutions in the public sector, where data protection obligations are easily identified. While the private sector comprises large and small businesses, determining who controls data is extremely difficult.

3. ACTORS AND THEIR ROLES

The complexity of data use, re-use and transfer is determined by distinct groups of actors. Despite the difficulty of anticipating the results of these actions or determining when an activity may have adverse implications, actors must take steps to prevent negative outcomes. The roles of actors must be clearly defined in the data protection legislation. It is crucial to outline the core requirements in the regulation and which actors would be accountable for ensuring compliance, adherence, and protection of individual rights. Given the importance of certain actors (e.g., controller, processor), it is vital to discern which function they have assumed concerning a specific processing activity. Protective measures taken by actors may unintentionally mistreat individuals or businesses by giving sensitive information to supervisory authorities or third parties.[118] Data protection authorities and courts have guided

[116] Available at: http://www.g7.utoronto.ca/trade/211022-digital.html; [Accessed on 12 January 2022];
[117] OECD (2002), *Mapping approaches to data and data flows - Report for the G20 Digital Economy Task Force,* (n 114);
[118] Van Alsenoy, B., (2016). *Regulating data protection: the allocation of responsibility and risk among actors involved in personal data processing*, p.293. Available at: https://www.researchgate.net/publication/308201270_Regulating_data_protection_the_allocation_of_responsibility_and_risk_among_actors_involved_in_personal_data_processing, [Accessed on 16 January 2022];

how to use the controller and processor concepts in practice.[119] This should be considered by those in the protection domain responsible for preventing or reducing such adverse outcomes of their efforts.

In the EU, the controller, joint controller, and processor roles are crucial for implementing the GDPR. They define who is accountable for adhering to specific data protection standards and, as a result, how individuals can safeguard their rights.[120] The GDPR defines a data *controller* as an entity (a natural or legal person, public body, etc.) that, alone or in collaboration with others, decides the objectives and means of processing personal data.[121] A controller is responsible for making important processing judgments. Controllership can be defined or derived from the facts of a case. When determining the mechanisms for processing and during the processing itself, the controller must use suitable technological and organisational precautions under GDPR's principles of lawfulness, fairness, transparency, data minimisation, accuracy, storage limitation, integrity and confidentiality.[122] This requirement relates to the amount of personal data collected, how it is processed, how long it is stored, and how it is accessible. Furthermore, such safeguards must ensure that personal data is not made available to an unlimited number of natural people by default without the individual's consent.[123] Data controllers conduct evaluations and provide appropriate safeguards before transferring personal data to a foreign country or an international organisation.[124] Moreover, they govern international transfers of personal data and create binding corporate rules authorised by supervisory authorities.[125] A *data processor* is an entity (a natural or legal person, public authority, etc.) that processes personal data on behalf of the controller. A contract or other legal act relating to a processor's processing of personal data must be in writing, including in electronic form. It must be legally binding to provide transparency and accountability. The controller and processor can design their contract with all required components or use standard contractual clauses.[126] Only processors that provide adequate guarantees will take appropriate technological and organisational measures to ensure that the processing complies with the

[119] Ibid;
[120] EDPB (2021), Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0, p.2. Available at: https://edpb.europa.eu/system/files/202107/eppb_guidelines_202007_controllerprocessor_final_en.pdf; [Accessed on 16 January 2022];
[121] Article 4(7) of the GDPR;
[122] Article 5(2) of the GDPR;
[123] Article 25. of the GDPR;
[124] Article 46. of the GDPR;
[125] Article 47(2) of the GDPR;
[126] EDPB (2021), Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0, (n 120), p.4;

GDPR's criteria and may be engaged by a controller. Expert knowledge, the processor's reliability and resources, and adherence to a standard or certification technique are all factors to consider.[127] In some cases, an entity can be both a data controller and a data processor. The GDPR also creates a framework for *joint controllers* and includes unique rules that govern their relationship.[128] Joint participation[129] can come from a prevalent decision made by all parties involved or from converging decisions.[130] Joint controllers are formed of two or more controllers who collaborate to determine the processing goals and techniques through an arrangement among themselves. Therefore, they decide on their specific responsibilities for compliance with the GDPR's requirements and emphasise the exercise of the data subject's rights and their respective duties.[131]

The CCPA utilises the terms businesses and service providers instead of controllers and processors. Despite their differences in wording, the concepts are the same. To be considered a *business* under the CCPA, a business must establish the aims and means of processing consumers' personal information[132], comparable to the GDPR's controller definition. The CCPA, in comparison to the GDPR, considers a company that does business in California if it meets one of the thresholds - the revenue of more than $25 million, data transactions involving 50,000 data subjects, or income derived from selling personal information accounting for 50% or more of the total revenue.[133] The *service provider* is an entity that processes information on behalf of a business and discloses consumer personal information for business purposes in line with a signed contract that prevents the receiving entity from retaining, using, or disclosing personal data for any other reason other than performing the service stipulated in the contract.[134] If a business is exempt from the CCPA's jurisdiction, any data it transmits to a service provider in California should be impacted. Service providers are only indirectly

[127] Ibid;
[128] Article 26. of the GDPR;
[129] See Case C-210/16, *Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein against Wirtschaftsakademie Schleswig-Holstein GmbH* ("Wirtschaftsakademie Schleswig-Holstein"), ECLI:EU:C:2018:388;
See Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, ECLI:EU:C:2019:629;
See Case C-673/17, *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2019:801;
See Case C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta*, ECLI:EU:C:2018:551;
[130] EDPB (2021), Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0, (n 120), p.3;
[131] Article 26 (1) of the GDPR;
[132] CCPA, Section 1798.140(c)(1);
[133] Ibid;
[134] CCPA, Section 1798.140(v);

affected by the CCPA. Also, within the CCPA, a requested party is defined as entities that are neither companies nor service providers.

In the PRC, a "*Personal Data Processor*" is defined as an entity (natural or legal) that autonomously chooses the aims and procedures of processing personal data.[135] This description is similar to the GDPR's definition of a data controller. Before interacting with entrusted parties, PIPL requires that Personal Data Processors have data processing agreements, which must be followed throughout personal data processing, and must have the Personal Data Processor's approval to pursue entrusting to other parties.[136] Unlike the GDPR, however, the PIPL does not specify whether this authorisation is general or must be requested from every Personal Data Processor each time the Trustee engages a new subcontractor. The rest of the requirements are comparable to those in the GDPR, except for the obligation to adopt categorised personal information management. Processors' personal information might be classified as part of security measures. Furthermore, if the data processor's processing of personal information surpasses a specific level, the data processor must employ individuals accountable for personal information security. The PIPL has not set such a value. This burden will be imposed on small data processors. However, particular levels and recommendations have yet to be defined.

II. LEGAL APPROACHES REGARDING DATA PROTECTION AND PRIVACY PRINCIPLES

Many nations have enacted data protection regulations and restrictions on cross-border data transfers. Creating data protection regulations began on a national level in the 1970s. Data protection became a regulatory concern due to privacy laws resulting in new legal obligations to give individuals control over their data. The right to privacy is recognised in many international instruments, including the Universal Declaration of Human Rights[137], the International Covenant on Civil and Political Rights[138], and regional ones such as the American Convention on Human Rights[139], the European Convention on Human Rights, the Charter of

[135] Article 73(I). of the PIPL;
[136] Article 21. of the PIPL;
[137] UN General Assembly(1948), Universal Declaration of Human Rights, (n.44), Article 12;
[138] UN General Assembly (1966), *International Covenant on Civil and Political Rights*, United Nations, Treaty Series, vol. 999, p. 171,Article 17.;
[139] Organization of American States (1969), *American Convention on Human Rights, "Pact of San Jose", Costa Rica*, Article 11.,;

Fundamental Rights of the European Union (hereinafter „CFR“)[140], the Arab Charter on Human Rights[141], the Asia-Pacific Economic Cooperation Privacy Framework and the Supplementary Act on Personal Data Protection of the Economic Community of West African States[142], etc.

Even though they are engaged with privacy, data protection laws emphasise personal data, setting rules and limitations for its processing rather than assessing privacy issues on a personal level. Data protection is essential to safeguard various rights and principles, from non-discrimination to freedom of expression, since the personal data processing is so widespread. From the world's first Data Protection Act of the German state of Hesse[143] and the decision of the Federal Constitutional Court of Germany on the Census Act[144], through the OECD Guidelines on the Protection of Privacy and Cross-Border Flows of Personal Data, as well as the Council of Europe Convention No 108 and its Protocols to the GDPR, they were progressively evolved into the data protection regulation.[145]

Initially, data protection regulations were primarily concerned with managing public data, including information about individuals. Nonetheless, the establishment of such legislation has focused on individual privacy rights that may be enforced. The creation and transfer of personal data have increased recently, causing procedures and data-sharing practices to change. In addition, a large number of national, regional, and worldwide privacy and data protection regimes have been enacted or amended. [146] When executing data processing activities, principles and data subject rights surrounding data protection are titled and formatted differently in various countries. Even if personal data is kept on any medium, not just digital data, data protection rights and principles are relevant for the digital environment.[147] Because data controls many areas of human lives, increased engagement through new and innovative data-intensive technologies poses a risk to data security and privacy. The growth of frameworks carries problems, such as ambiguity, which arise when frameworks collide. The national implementation structure differs between two approaches, both *comprehensive* and *limited*. A

[140] Charter of Fundamental Rights of the European Union, 2016/C 202/02,;
[141] League of Arab States. (2004). Arab Charter on Human Rights. League of Arab States, Article 16(8);
[142] ECOWAS (2010), ‘Supplementary Act on Personal Data Protection within ECOWAS’ ;
[143] Hesse Data Protection Act (1970) [“Hessisches Datenschutzgesetz 1970“] , Gesetzund Verordnungsblatt für das Land Hessen (HE GVBI), , nr. 41, Part I, p. 625-627,]
[144] BVerfG, Urteil des Ersten Senats vom 15.Dezember1983- 1 BvR 209/83-,Rn.1-215;
[145] Doneda D.(2022), Guidelines for judicial actors on privacy and data protection, UNESCO,p.15. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000381298; [accessed 23 February 2022];
[146] OECD (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, p.164. Paris, Available at: https://doi.org/10.1787/bb167041-en. [Accessed 20 January 2022];
[147] Ibid, p.18;

comprehensive approach with similar privacy principles has been used in the private and public sectors. In contrast, the limited approach only applies to the public sector with explicitly defined data privacy principles. A comprehensive approach strikes a balance between people's private interests and the objectives of the state and industry. Consent is the primary legal foundation for data collection, processing, and transfer under this strategy. With a limited approach, privacy protection is directed by industry self-regulation and consumer needs.

1. THE EUROPEAN UNION

The right to the protection of personal data is a fundamental right in the EU, which is incorporated in Article 8. of the CFR and Article 16 (1). of the Treaty on the Functioning of the European Union[148]. Furthermore, the right to protect personal data is inextricably linked to the private and family life of a person, his/her home, and his/her correspondence, as stated in Article 7. of the CFR.[149] In 1970, the Hessian Parliament passed the world's first comprehensive data protection legislation in Wiesbaden, Germany. Other German states followed, and federal legislation was enacted in 1977.[150] The first binding international regulation on data protection was the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data which the Council of Europe adopted in 1981. This Convention aims to ensure that individuals, regardless of nationality or residence, have their rights and fundamental freedoms respected in each signatory country, particularly their right to privacy concerning the automatic processing of their personal data in public and private sectors.[151] In addition, Convention No.108 establishes rules for sensitive data[152], data security[153], and extra data subject protections[154]. For years, EU law has contained a threshold test for cross-border data flow and a legal foundation prohibiting data exports to countries that do not fulfil this requirement.

---

[148] Consolidated Version of the Treaty on the Functioning of the European Union, , 2012/C 326/01;
[149] The CJEU held in *Schencke and Eifert v Hessen* joined cases, that Art. 8 of the EU Charter is intrinsically related to Art. 7 of the Charter, which underlines the right to respect for private life. In reference to the processing of personal data, Articles 7 and 8 of the Charter affirm the right to respect private life. This right extends to any information about a person who can be identified or identified.See *Schencke and Eifert v Hessen, Joined Cases C-92/09 and C-93/09 (9.11.2010)*, ECLI:EU:C:2010:662, paragraphs 47. and 52;
[150] Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG), Bundesgesetzblatt Jahrgang 1977 Teil I Nr. 7, ausgegeben am 01.02.1977, Seite 201, 8.;
[151] Article 1. of the Convention No.108;
[152] Article 6. of the Convention No.108;
[153] Article 7. of the Convention No.108;
[154] Article 8. of the Convention No.108;

The EU's first adopted binding data protection regulation that all EU member states followed was the Data Protection Directive (hereinafter „DPD"). The DPD defined the basic principles for the lawfulness of data processing and the data subjects' rights and independent supervisory authorities in the Member States. Member States were obliged to harmonise their regulations to allow intra-EU transfers without additional procedures, and for international data flows, DPD introduced an adequacy requirement.[155] This Directive was reinforced by the ePrivacy Directive[156], which aimed to unify national legislation of the Member States on the protection of the right to privacy, particularly in the context of the processing of personal data in electronic communications networks. The ePrivacy Directive was amended by the Data Retention Directive[157], whose goal was to ensure that electronic communications data is retained for investigating and prosecuting serious crimes, such as organised crime and terrorism. However, the Data Retention Directive was invalidated by the judgements of the Court of Justice of the EU (hereinafter „CJEU") in the cases of *Digital Rights Ireland and Seitlinger*[158]. The CJEU ruled that the Data Retention Directive involves serious interference with rights to respect for private and family life under Article 7. of the CFR and personal data protection under Article 8. of the CFR, while this interference was not rigorously limited to what is strictly required.[159] The EU updated its entire legislative framework to ensure data privacy. It enacted the GDPR, which repealed Directive 95/46/EC and Directive (EU) 2016/680[160] on the protection of personal data in criminal proceedings. Furthermore,

[155] Article 45-46. of the DPD;
[156] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p.37,;
[157] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the European Union L 105, 13.4.2006., pp. 54-63;
According to Article 5 (1). of the Data Retention Directive, data such as numbers or user names, date, time, and length, as well as the subscriber's international mobile subscriber identification and location via Cell ID for mobile phones, must be kept by electronic communications service providers to identify the source and destination of fixed network and mobile telephony, all to investigate and prosecute severe crimes defined by national legislation.
[158] See *Digital Rights Ireland and Seitlinger and Others Joined Cases C-293/12 and C-594/12, EU: C:2014:238*;
[159] CJEU (2020), *Fact Sheet – Protection of personal data*, Available at: https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/fiche_thematique_-_donnees_personnelles_-_en.pdf; [accessed 27 February 2022];
[160] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016, L 119, p. 89);

Regulation (EC) No 45/2001[161] enabled the European Data Protection Supervisor to be established in EU institutions and organisations processing personal data. However, Regulation (EU) 2018/1725[162] created a new regulatory framework in this field. The GDPR lays down standardised rules across the EU to give a uniform approach to personal data protection.[163] The GDPR's two objectives are the same as those of the Data Protection Directive. It aims to preserve natural people's fundamental rights and freedoms, including their right to personal data protection. It will not restrict or prohibit the free movement of personal data within the EU[164]. The ePrivacy Regulation, intended to replace the e-Commerce Directive, governs the use of electronic communications services inside the EU. The ePrivacy Regulation is directed mainly at businesses in the digital economy, and it defines additional rules for processing personal data that they must follow. The ePrivacy Regulation will supplement the GDPR's basic standards on personal data processing by providing particular regulations governing electronic communications. As a result, in cases where both laws apply, the ePrivacy Regulation will take precedence over the GDPR.

The European Commission has declared 2020–2030 as Europe's "*digital decade*", with the challenge of preserving EU technological and digital sovereignty. As part of the EU digital decade, the European Commission issued various laws to strengthen digital sovereignty, externalise standards by controlling internal market access, and increase integration by offering guidance on digital difficulties. The EU changed its policies to guarantee the data sovereignty of its individuals and businesses as the digital economy expanded and the personal data of individuals became an unlimited resource. The EU Network and Information Security Directive (hereinafter „NIS Directive“)[165], which governed access to the internal market and established international cyber standards, was the first step in building a unified EU digital policy. The EU Cybersecurity Act[166] of 2019 provides a framework for cybersecurity

[161] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001, L 8, p. 1);
[162] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018, on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC;
[163] CJEU (2020), *Fact Sheet – Protection of personal data*, (n.159), p.2;
[164] Article 1. of the GDPR;
[165] 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,*OJ L 194, 19.7.2016, p. 1–30*;
[166] 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), PE/86/2018/REV/1, *OJ L 151, 7.6.2019, p. 15–69*;

certification for information and communications products and services. Moreover, the European Commission released Recommendations for cybersecurity of 5G networks[167] and a "toolbox"[168] that includes tight access controls on secure 5G networks.

The Data Governance Act of 2021 establishes the methods and structures for businesses, individuals, and the public sector to share data. The risk-assessment system to govern internal market entry was introduced by the Artificial Intelligence Act of 2021 (hereinafter „AI Act“)[169]. The Digital Services Act (DSA)[170] and the Digital Markets Act (DMA)[171] were enacted to tackle concerns raised by launching innovative products and services into the digital market. The EU proposed the legislation in December 2020, and a political agreement was obtained on the DMA on March 25, 2022, and for the Digital Services Act on April 23, 2022[172]. They build a unified set of new laws that will apply across the EU to promote a fair playing field to enhance innovation, growth, and competition to create a safer digital world in which the fundamental rights of all users of digital services are respected. Furthermore, the European Commission issued the Data Act[173] on February 23, 2022, proposing new regulations for who can use and access data created in the EU across all economic sectors and under what circumstances data may be used to produce value. The EU Chips Act [174]of 2022 represents a strategy to combine national efforts into a cohesive European semiconductor research plan and secure the EU's supply security, resilience, and technical leadership in semiconductor technology and applications.

2. THE UNITED STATES OF AMERICA

The United States of America has not been a big proponent of data protection, preferring to use a sectoral strategy that combines law, regulation, and self-regulation by

[167] EC Recommendation of Cybersecurity of 5G networks, C(2019) 2335 final;
[168] EC (2020), Cybersecurity of 5G networks EU Toolbox of risk mitigating measures CG Publication;;
[169] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final;
[170] Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/ECCOM/2020/825 final;
[171] Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM/2020/842 final,;
[172] More information is available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package; [accessed 16 February 2022];
[173] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM(2022) 68 final 2022/0047 (COD);
[174] Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act), COM(2022) 46 final 2022/0032 (COD);

businesses. Although the U.S. Constitution does not expressly mention data protection, the First and Fourth amendments provide privacy rights. The First Amendment protects privacy by safeguarding freedom of association and limiting information privacy. Since their impact on the data processor's speech, rules restricting information sharing on privacy concerns are subject to constitutional challenge.[175] The Fourth Amendment protects from searches conducted without warrants or the seizure of persons or property. What a person intentionally discloses to the public is not protected under the Fourth Amendment, even in his or her own home or business. But anything he or she wants to keep private, even in a public location, might be legally protected.[176] As a result, anything is private if it is entirely secret, and this known as the secrecy paradigm. Furthermore, the reasonable expectation of the privacy test has become an essential part of the Fourth Amendment's analysis. This test examines whether the government's activity violated the individual's reasonable expectations of privacy. This test has two parts:

1. The person showed an actual (subjective) expectation of privacy;
2. The society is willing to recognise expectations as reasonable.

For the Fourth Amendment to be violated, both conditions must be fulfilled. However, there are several exceptions (for example, the federal Fourth Amendment protection does not extend to government intrusions and open field data gathering, etc.). The protection of privacy in the United States has gone a long way, and privacy legislation in the United States has improved significantly. From this U.S. Supreme Court decision recognising that the right to privacy is protected by the U.S. Constitution against certain forms of government intrusion, to the U.S. Congress implementing the Privacy Act[177] to highlight the privacy risks posed by public records, to U.S. states enacting sector-specific laws requiring data breach notification and information security requirements[178]. In recent years, the U.S. has found a middle ground between its privacy commitments and its position as a global leader in digital development. As a result, the regulatory strategy has been flexible, focusing on private litigation and sector-specific privacy legislation[179].

[175] See case of *Sorrell v. IMS Health Inc.* 131 S. Ct. 2653 (2011);
[176] The Fourth Amendment protects persons, not locations, according to case of *Katz v. United States, 389 U.S. 347 (1967)*. paragraph 351;
[177] Privacy Act, 5 U.S.C. § 552a (1974);
[178] Alan C. R. (2020),*" The Privacy, Data Protection and Cybersecurity Law Review"*, Sixth Edition, p.399. Available at: https://datamatters.sidley.com/wp-content/uploads/2019/11/The-Privacy-Data-Protection-and-Cybersecurity-Law-Review-Edition-6.pdf [accessed 11 March 2022];
[179] Ibid,p. 400;

Although there is no comprehensive federal legislation affecting data protection, there are a variety of sector-specific data protection regulations at the federal and state levels. For example, the HIPAA, as amended by the Health Information Technology for Economic and Health Act (hereinafter "HITEHA")[180] regulates health insurance at the federal level and includes data privacy and security. HIPAA's data protection section consists of the Security Rule and the Privacy Rule for data confidentiality standards. The COPPA governs the collection of personal data from minors, prohibiting the collection of PII from children under the age of 13 online or through digitally connected devices unless there is verifiable parental consent and mandatory publication of privacy notices. The GLBA safeguards non-public personal information, essentially PII, except for publicly available financial data (e.g. mortgage information). The VPPA governs the dissemination of information concerning video content usage by consumers. The Fair Credit Reporting Act (hereinafter "FCRA")[181] is federal legislation that regulates the acquisition of credit information from consumers and the activities of credit reporting companies. However, it is primarily self-regulated at the federal level. The U.S. data protection regulations do not impose restrictions on international data transfers[182].

Furthermore, entities that are not subject to sector-specific laws are subject to the U.S. Federal Trade Commission (hereinafter "FTC") jurisdiction. This privacy regulator deals with data privacy and information security issues.[183] In January 2020, California passed the first comprehensive data protection law in the U.S., i.e. California Consumer Privacy Act[184]. The goal of the CCPA is to regulate the collection of PIs from California residents and provide residents with broader privacy rights concerning access and sharing PI.

The CPRA was adopted to amend and expand the CCPA. The CPRA provides distinct requirements and restrictions for using sensitive personal data and strengthening privacy rights while also introducing rights to correct and opt out of automated decision-making technologies. At least fifteen state legislatures (e.g.Arizona, Florida, Minnesota, and Washington) have confirmed that they would adopt CCPA-style consumer privacy legislation. Also, the Hacking Stop and Improving Electronic Data Security Act (hereinafter "SHIELD Act")[185], passed in

[180] Health Information Technology for Economic and Health Act, Pub.L.No.111-5,123 Stat.226;
[181] Fair Credit Reporting Act,12 U.S.C. §§1830-1831(1970) 15 U.S.C. §1681 et seq.(1970);
[182] Schwartz, P. M., (2013), The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures. 126 Harvard Law Review 1966, UC Berkeley Public Law Research Paper No. 2290261, p.1977.Available at SSRN: https://ssrn.com/abstract=2290261; [Accessed on 13 January 2022];
[183] Section 5 of the Federal Trade Commission Act,15 USC 45;
[184] California Consumer Privacy Act, Cal. Civ. Code, paras 1798.100–1798.199;
[185] The Hacking Stop and Improving Electronic Data Security Act, S.B. 5775, Reg.Sess.2019-2020 (N.Y.2019);

New York, regulates companies that manage PIs when developing data security programs with adequate administrative, technological, and physical safeguards.

Moreover, the Uniform Law Commission of the United States finished its version of the legislation in 2021, which any state can embrace. The Commission passed the Uniform Personal Data Protection Act (hereinafter "UPDPA"), which is mainly equivalent to legislation passed by California, Virginia, and Colorado. The UPDPA imposes data protection regulatory duties on personal data held in a system of records that a business uses to collect data about individuals in order to deliver personalised communications or for other reasons. It is based in part on the federal Privacy Act of 1974.

Additionally, the United States courts have recognised privacy torts in line with the Restatement (Second) of Torts[186]. A lawsuit can now be launched on behalf of aggrieved parties for invasion of privacy, public disclosure of private information, and infringement of the right of publicity or personal image, among other things.

3. THE PEOPLE'S REPUBLIC OF CHINA

Before entering into force the Personal Information Protection Law and Data Security Law in the fall of 2021, the PRC did not have a compressive data protection law. However, the PRC had sectoral laws that contained only a few sentences regarding data protection, such as Cybersecurity Law[187], The Civil Code, Data Security Law, and e-Commerce Law[188]. The Constitution of the PRC does not mention data protection but only mentions privacy in Article 40. Furthermore, a significant part of the PRC data protection was defined by Tort Liability Law. The said Law emphasises the right to privacy as a part of protected civil rights and interests[189]. However, the PRC's most critical piece of legislation aimed at solving data protection issues before the PIPL is the Decision on Internet Information Protection (known as the 2012 SC-NPC Decision), which aims at regulating electronic information and protecting individuals' privacy. The PRC's complex legal system allows provinces, regions, and cities to introduce data protection laws[190] or specific provisions into existing regulations[191].

[186] Restatement (Second) of Torts, §652A (Am. Law Ins.1977);
[187] Cybersecurity Law of the People's Republic of China No.53 (2016);
[188] E-Commerce Law of the People's Republic of China No.7 (2018);
[189] Article 2. of the Tort Liability Law;
[190] Jiangsu Provinces Regulation of Information Technology and Xuzhou Citys Municipal Provisions for Computer Information System Security protection.
[191] Shanghais Consumer Protection Rules and Henan Provinces.

The PIPL applies to all actions in the PRC, including data subjects' personal information and activities outside PRC that offer services and goods in the PRC.

The minimum requirements that must be met for the collection and protection of personal data are prescribed as follows:[192]

1. establishment of procedures for the protection of PI;
2. establishment of advanced technological solutions for PI security;
3. conducting a risk assessment before undertaking any PI-related activities;
4. in case of high-risk situations, utilising a risk-based approach in a case exposing minimum requirements.

Furthermore, consent is essential for managing personal information, particularly sensitive personal information. In addition to consent, the PIPL specifies more burdensome regulations that must be followed. There are several exceptions to these norms, such as legislative obligations, conveying news of broad interest, etc. If a particular quantity of personal information is collected, the data handler is required to deploy an information protection officer to manage and secure the data correctly. It is even feasible to determine where data is stored. This recently enacted regulation mandates the use of encryption when sending information to other parties in the PRC or overseas.

One of the essential aspects of the PIPL is its extraterritorial effect, which implies that the PRC authorities have legitimacy even outside the country's borders. In other words, they have the power to protect the personal information of their citizens who are prosecuted in any country. Even though a large proportion of data processing for individuals occurs within the country's boundaries, it may sometimes happen outside the country. However, it should only be done to provide merchandise to citizens, investigate individual behaviour in the PRC, and in other situations prescribed by law. Businesses with headquarters outside of the PRC should set up a separate entity to conduct business in the country and hire an agent from PRC to supervise all data-gathering operations. It should be highlighted that companies that process PI are required to have an internal audit to determine the amount of risk, all to avoid illegal activity with the transferred data[193]. When sharing personal information across borders, it must be verified that the foreign recipient has at least the same degree of protection as the PIPL. These additional restrictions are still enforced based on the sensitivity of the data and its volume.

[192] Available at: https://www.accountablehq.com/post/chinas-personal-information-protection-law; [Accessed on 02 January 2022];
[193] Article 54. of the PIPL;

Although essential differences exist, the PIPL is comparable to the EU GDPR. This is apparent mainly in the government's handling of personal data. Although the PIPL regulates this sector, a few exceptions exist, such as public safety and national security concerns. The PIPL establishes the responsibilities of international corporations' and requires from those not based in the PRC to hire a local representative who will act as an agent in resolving issues relating to personal data gathered in the PRC.

The Data Security Law (hereinafter "DSL")[194] creates a system for categorising information gathered in the PRC into core data and important data. Core data is defined as information critical to national and economic security, the residents' well-being, and substantial public interest under this regulation. National, regional, and sectoral authorities, on the other hand, are in charge of defining the Important data.

Regardless of the sensitivity level of the content or whether the data was obtained in the PRC, both CIIOs and non-CIIOs are barred from disclosing any data stored in the PRC to any foreign judicial or law enforcement organisation without the prior authorisation of the PRC authorities. The DSL mandates firms doing business in the PRC to build and improve their data security systems, take remedial action when data security flaws are discovered, and inform users and authorities of any data breaches as soon as possible. Companies that handle at least "critical data" must appoint a data security officer or management team and submit risk assessments to the PRC authorities.

The PRC's Cybersecurity Law has mandated cybersecurity assessments for critical information. The section of this Law dealing with the clarification and extension of data localisation and requirements for transmitting core and critical data is the most relevant section. For example, Critical Information Infrastructure Operators ("CIIOs") that handle data from information networks, infrastructure, and natural resources must verify that it is created and stored in the PRC. A security self-assessment is undertaken before the data is transferred outside the PRC's borders.[195]

There is still a scarcity of case law concerning data or privacy protection in the PRC. In the absence of legislated requirements, the PRC judicial system has produced a succession of ground-breaking rulings to define privacy in law. These pioneer rulings, are the *Qi Yuling v Chen Xiaoqi* regarding identity theft, the case of the *Wang Fei* concerning online shaming and the *Shanghai Roadway* regarding criminal prosecution. The prosecution is the main course of

[194] Data Security Law of the People's Republic of China No.84;
[195] Article 35. of the Cybersecurity Law;

action for citizens seeking to preserve their right to personal information. There are also certain civil cases available under the Tort Liability Law.[196]

4. DEVELOPING COUNTRIES

Most developing countries claim to have at least a draft of the data protection framework at the national level. Some nations have adopted a sufficient level of legislation restrictions to deter illegal acts, with varying degrees of effectiveness, whilst those lacking comprehensive data protection and privacy regulations struggle to punish violators adequately. Although it is important that developing countries have national, regional and global data protection policies and regulations to prevent data misuse and increase their benefits, 15% of countries worldwide do not have data protection and privacy laws (including Venezuela, Cuba, Syria, Libya, etc.).[197]

The motivations for governing data protection may differ depending on a country's political, economic, social, technical, and cultural values and ideological backgrounds. Some of the primary policy objectives are to promote domestic economic growth, maximise the socioeconomic advantages of data-driven technologies, solve severe public concerns such as privacy violations, and minimise cybersecurity risks.[198] The EU, the U.S., and the PRC aspire to exert influence over other countries through trade agreements, development and improvement of methods and resources required to survive in a rapidly changing environment or in exchange for market access. Smaller or less developed nations would probably feel driven to choose one realm over the others, either because they already have significant economic contact with that market or because they favour that realm's data control policy. Many countries find selecting between the two domains challenging since they have substantial economic links.[199] As a result of their economic interests being linked with these blocs, Latin American states are frequently forced to choose between the GDPR and U.S. models. Several African countries appear to be aligning with the PRC data sovereignty model, but they also have ties to

[196] Papakonstantinou, V. & Hert, P.. (2015). *The Data Protection Regime in China. In-Depth Analysis*, Brussels Privacy Hub Working Paper, Volume 1, Number 4, Available at: SSRN: https://ssrn.com/abstract=2773577 ; [29 January 2022];
[197] Available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide; [Accessed on 15 February 2022];
[198] UNCTAD (2021), *Digital Economy Report - Cross-border data flows and development: For whom the data flow*, United Nations Publications, (n 2), p.119;
[199] Ibid, p.116;

the EU and the United States. The PRC has a more significant influence on some emerging Asian countries.[200]

The Law on Personal Data Protection governs data protection in Bosnia and Herzegovina, one of the world's developing countries. Under the Stabilization and Association Agreement, Bosnia and Herzegovina has agreed to align its domestic legislation with the acquis communautaire. However, due to the complex political situation, the revised Law on Personal Data Protection consistent with the GDPR has yet to be implemented.

In line with the GDPR, Brazil enacted the comprehensive Brazilian General Data Protection Law[201] in 2020. The Federal Constitution, the Brazilian Civil Code, and laws and regulations dealing with specific types of relationships (e.g., Consumer Protection Code[202]); which regulate individual sectors (e.g., financial institutions); and special professional activities all contain data protection provisions and principles. Furthermore, regulations govern the government's and public entities' handling and security of information.[203]

In addition, India also lacks comprehensive data protection and privacy legislation. The Indian Data Protection and Privacy Framework are represented by the Information Technology Act[204] of 2000 and the Information Technology Rules (Privacy Rules) of 2011[205]. A draft law on personal data protection, the Personal Data Protection Bill 2019 (hereinafter "PDP Bill")[206], was created in 2019 and relies to a limited extent on the EU GDPR. A joint parliamentary committee composed of members of both houses of the Indian parliament is currently considering the PDP Bill. Although India is not a signatory to any personal data protection conventions, it is a signatory to other international declarations and conventions that acknowledge the right to privacy, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights.[207]

---

[200] Ibid;
[201] Brazilian General Data Protection Law, Federal Law no. 13.709/2018 (or A *Lei Geral de Proteção de Dados* Pessoais (*LGPD*), Lei n° 13.709/2018);
[202] Consumer Protection Code, Federal Law No. 8.078/90;
[203] Available at: https://www.dlapiperdataprotection.com/?t=law&c=BR; [Accessed on 21 January 2022];
[204] Information Technology Act, 2000 (21 of 2000);
[205] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules), THE GAZETTE OF INDIA [PART II-SEC. 3(i)];
[206] The PDP Bill proposes a legal framework to protect individuals' autonomy concerning their data, specify where the flow and usage of personal data are appropriate, the rights of individuals, establish standards for cross-border transfers of personal data, etc.
[207] Bentotahewa, V., Hewage, C. & Williams, J. (2022), The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries. *SN COMPUT. SCI.* 3, 183, Available at: https://link.springer.com/article/10.1007/s42979-022-01079-z ; [Accessed on 13 March 2022];

In the Philippines, data privacy is governed under the Data Privacy Act, commonly known as Republic Act No. 10173[208]. The Act aims to protect the fundamental human right to communication privacy while permitting the free flow of information to stimulate innovation and growth. The Philippine House of Representatives enacted and transmitted to the Philippine Senate a bill to amend the Act in 2021.

5. PRIVACY FRAMEWORK

Privacy is challenging to attain, mainly since it is a process that guides the protection of fundamental aspects, and the ways to accomplish it may differ. Due to privacy's broad and different nature, it is more difficult for businesses and individuals to interact, which can have significant implications for individuals and repercussions for businesses' products and growth prospects. Additionally, businesses are subject to increasing privacy laws, requiring appropriate technical and organisational measures, but it is not specified which certain steps must be performed to meet these criteria. In this case, the privacy framework can help create privacy and security strategies that make compliance more attainable. It represents a set of guidelines or standards that serve as the foundation for an organisation's privacy program. It aims to meet the needs of a businesses by satisfying compliance requirements and encouraging monitoring and development.

Regarding privacy risk management on the international level, the International Electrotechnical Commission (hereafter „ICE“), in collaboration with the United States National Institute of Standards and Technology (hereafter „NIST“), and the International Organisation for Standardization (hereafter „ICO“) are crucial players. ISO and IEC are international non-governmental organisations, whereas NIST is a non-regulatory government agency within the U.S. Department of Commerce.

The EU has also recognised three private international nonprofit organisations responsible for developing and defining standards and guidelines. They cooperate with the Cybersecurity Agency of the European Union. The European Telecommunications Standards Institute encompasses a wide range of sector-specific privacy standards. The European Committee for Standardization and the European Committee for Electrotechnical Standardization collaborate to create European privacy information management systems. The ePrivacy Directive and the GDPR are the two essential components of the EU's data protection

[208] Data Privacy Act of 2012 (Republic Act No. 10173);

legal framework. The APEC Privacy Framework defines privacy principles and guidelines in Asia, providing a foundation for the APEC Cross-Border Privacy Rules, a regional approach. The OECD Privacy Framework – the first international consensus on privacy protection in the context of the free flow of personal data – served as the foundation for these frameworks. Despite existing standards and frameworks, there are national privacy standards, and numerous businesses design their privacy frameworks.

5.1. FAIR INFORMATION PRACTICE PRINCIPLES

In the 1970s, Fair Information Practice Principles (hereafter "FIPPs") initially emerged in some of the world's first data privacy legislation and government publications. The word "FIPPs" originally appeared in a 1973 study by the Advisory Committee on Automated Personal Data Systems for the Secretary of the United States Department of Health, Education, and Welfare (hereinafter "HEW")[209]. The core concept of FIPPs was developed in response to the computer traffic concerns of huge organisations attempting to acquire, use, and divulge personal information. Laws based on the FIPPs, such as GDPR, purportedly provide individuals control over data collection and processing. The FIPPs are designed to guarantee that data subjects.

1. are aware of the fact that their data is being collected; and
2. to give their consent to certain practices.

Due to growing privacy issues about electronic sources retained in the public and private sectors, the HEW report entitled Records, Computers, and Citizens' Rights[210] recommended the FIPPs as a principle for protecting the privacy of the data in record-keeping systems. Transparency, usage limitation, access and correction, quality of data, and security were among the basic fair information principles proposed in the HEW report, which had appeared in dispersed regulations and reports around the globe. The FIPPs are a recognised framework at the centre of the 1974 Privacy Act and are reflected in the rules among many U.S. states, foreign countries, and international organisations.

[209] Hartzog, W. (2017) 'The inadequate, invaluable fair information practices,' *Maryland law review (1936)*, 76(4), p. 957. Available at: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3017312_code1107005.pdf?abstractid=3017312&mirid=1; [Accessed on 28 January 2022];

[210] US Department of Health, Educ. & Welfare, (1973), *Records, Computers And The Rights Of Citizens: Report Of The Secretary's Advisory Committee on Automated Personal Data Systems*, no. (Os)73-94, Available at: https://www.justice.gov/opcl/docs/rec-com-rights.pdf; [Accessed on 28 January 2022];

However, they were not fully acknowledged until the Organisation for Economic Cooperation and Development ("OECD") formally approved them in its Guidelines on Privacy and Transborder Flows of Personal Data in 1980.[211] The widespread acceptance of FIPPs-based regimes enabled the implementation of the EU's data protection legislation based on the FIPPs and forbade data transfers to jurisdictions lacking adequate data protection. The FIPP countries can use as many or as few as they want. The U.S. is probably the most well-known country with only partially integrated FIPPs in its privacy regime. The FIPPs, for example, include U.S. privacy legislation such as the HIPAA and the U.S. FTC regulation of privacy, primarily through the FTC's power to prosecute unfair and deceptive trade activities.

Almost every other government that has recognised privacy has adopted the FIPPs as the core substantive data protection. Of course, there are drawbacks to this severability. While the FIPPs remain generic principles with uncertain proportionality criteria, they focus on particular difficulties to obtain more objective estimates of privacy than simply instinct while preserving compatibility with commonly believed traits like autonomy and fairness. Global digitalisation requires some degree of coherence between privacy regimes. It is necessary to agree on the limitations of data collection and use.

Therefore, the FIPPs represent a shared understanding of best data practices and have proven highly adaptable. A global privacy language opens the door to major diplomatic solutions for safeguarding privacy in the global digital economy (e.g. the E.U.-U.S. Privacy Shield).

5.2. THE OECD GUIDELINES

The Organisation for Economic Cooperation and Development (hereinafter "OECD") issued revised guidelines in 2013 establishing privacy protection and transborder flows of personal data that enhanced the OECD's initial guidelines[212] from 1980, which became the first set of internationally recognised privacy principles to endorse integration. The OECD used the U.S. Department of Health, Education, and Welfare's fair information principles in 1980 to develop a set of eight Fair Information Practices codified in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Today, the OECD Guidelines

[211] Hartzog, W. (2017) 'The inadequate, invaluable fair information practices, (n 209), p. 957;
[212] These guidelines were updated in 2013 and in 2019. More information is available at: https://www.oecd.org/sti/ieconomy/privacy.htm.; [Accessed on 17 January 2022];
OECD(2013), "Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,", Paris.

serve as the foundation for most of the privacy legislation in the world. They establish basic data protection requirements to maintain the fundamental but competing features of privacy and the free flow of information. Their primary condition is that the collection and use of personal data be either explicitly permitted by law or consented to by the individuals to whom the data pertains and limited to the minimum collection and use required to achieve the stated purpose. According to the OECD Guidelines, personal data must be protected, reasonably accessible, and handled transparently and accountable.[213]

The OECD Guidelines have been revised to include basic alterations essential for protecting individual privacy while avoiding potential constraints on the use and personal information that are becoming progressively significant. The revised guidelines generate a considerable difference between principles that apply to data collection and those related to data use or other processing activities to move data protection away from individuals and concentrate on data use rather than data collection. [214] When deciding if specific data usage should be allowed, weighing the advantages and disadvantages of data usage and the safeguards to protect against harmful impacts is necessary.

The revised principles apply only to personal data that has not been "de-identified."[215] The guidelines provide directions to enhance coherent domestic methods for resolving data security risks in a highly interconnected society. The Guidelines reinforce the inclination to foster a security culture as a community's daily routine when using Information and Communication Technologies (hereinafter "ICTs") and undertaking online activities.

5.3. APEC PRIVACY FRAMEWORK

The Asia Pacific Economic Cooperation Privacy Framework (hereafter APEC Privacy Framework) is a set of principles and implementation guidelines designed to achieve appropriate privacy protections and the free flow of information in the Asia Pacific region while adhering to national legal requirements, relevant international frameworks for privacy protection, and ensuring ongoing economic growth in the APEC region.[216] The APEC Privacy

[213] Cate, Fred H.; Cullen, Peter; and Mayer-Schonberger, Viktor, "Data Protection Principles for the 21st Century" (2013). *Books & Book Chapters by Maurer Faculty*. p.5. Available at: https://www.repository.law.indiana.edu/facbooks/23, [Accessed on 28 January 2022];
[214] Ibid, 11;
[215] Ibid, 12;
[216]Asia-Pacific Economic Cooperation, APEC PRIVACY FRAMEWORK (2015) Available at: https://www.apec.org/docs/default-source/publications/2016/11/2016-cti-report-to-ministers/toc/appendix-17-updates-to-the-apec-privacy-framework.pdf?sfvrsn=8152a06c_1; [Accessed on 28 January 2022];

Framework, which helps enhance e-commerce across the Asia Pacific region, is coherent with the OECD's Guidelines and confirms the importance of privacy to individuals and the information society.

Furthermore, the APEC Privacy Framework initiated the development of the APEC Cross-Border Privacy Rules system (hereinafter „CBPR system“). The APEC Cross Border Privacy Rules System is a voluntary accountability-based system developed to support privacy-respecting personal information flows among APEC economies. The CBPR system aims to create a regional approach across APEC economies, each of whose are at a different stage of implementing the Privacy Framework. The CBPR system's formation underlies the objectives of APEC and the Privacy Framework.[217]

To join the CBPR system, each APEC member economy should select one government enforcement agency and one third-party accountability agent to ensure participants' adherence. Also, businesses that comply with the CBPR system are technically subject to a single privacy system Privacy Framework for data transfers between APEC economies that have entered the CBPR system. Nevertheless, since the CBPR system does not substitute domestic laws, businesses must comply with domestic privacy laws that impose stricter standards. As a result, while the CBPR mechanism establishes a baseline for privacy, the compliance gains for businesses differ.

Even though the APEC Privacy Framework and the GPDR are based on the OECD privacy principles proposed in 1980, the CBPR persists attached to the OECD's free-trade principles, while the EU privacy framework has progressed with the EU Data Protection Directive and later with the GPDR. The GDPR is a legally binding framework that enforces an EU data privacy regime for data handled by EU citizens.

The CBPR framework, on the other hand, is a voluntary, principles-based accountability framework that includes an accountability agent to try and solve consumer concerns and disputes. Violations of the CBPR framework encompass the requirement for a consumer in an APEC member economy to file a complaint with the accountability agent in

[217] Raul,A.C. (2014), The Privacy, Data Protection and Cybersecurity Law Review, Law Business Research Ltd, London, p.24. Available at: https://www.sidley.com/~/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/apec-overview/fileattachment/apec-overview.pdf; [Accessed on 30 January 2022];

the jurisdiction where the business is based. Following an investigation, the accountability agent participates in dispute resolution with the individual[218].

5.4. NIST PRIVACY FRAMEWORK

The National Institute of Standards and Technology (hereinafter "NIST") issued a Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management (hereinafter „NIST Privacy Framework“)[219] to ensure optimal privacy design activities that promote privacy by design fundamentals and enable businesses to safeguard their individuals' privacy. This voluntary instrument was developed across open, consensus-based procedures encompassing private and public relevant parties.

The Privacy Framework aims to empower businesses to deal with privacy threats by thinking about privacy as individuals organise and implement mechanisms, objects, and services that affect the people, engage in their privacy policies, and uplift cross-organisational workforce cooperation throughout the data processing ecosystem. Therefore, the Privacy Framework is adaptive sufficiently to resolve broad privacy necessities, empower more innovative and efficient approaches that can produce positive results for individuals and businesses, and keep engaged with the latest innovations such as artificial intelligence and the Internet of Things, thanks to risk outcome-based approach.

There are three sections: the Core, Profiles, and Implementation Tiers. Each element improves privacy risk management by connecting business and privacy protection strategies.

The Core[220] is a set of privacy protection activities and outcomes that enable interaction of priority privacy protection procedures and effectiveness. The Core is further subdivided into crucial Categories and Subcategories for every Function. Functions organise necessary privacy actions while helping a business articulate its privacy risk management by managing data processing, empowering risk management decisions, deciding how to engage with people, and enhancing by looking at previous acts. The five Functions, Identify-P, Govern-P, Control-P, Communicate-P, and Protect-P, are a method of reducing the privacy risks associated with data processing[221].

---

[218] Ibid;
[219] Boeckl, K. and Lefkovitz, N. (2020), NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0, Other, National Institute of Standards and Technology, Gaithersburg, MD, [online],Available at: https://doi.org/10.6028/NIST.CSWP.01162020; [Accessed on 30 January 2022];
[220] Ibid,p.6;
[221] Ibid,p.7;

- Identify -P's responsibility is to mitigate the risks associated with cybersecurity-related privacy incidents (e.g., privacy breaches).
- Govern-P Function concentrates on organisational-level activities like creating organisational privacy values and policies, recognising legal standards, and understanding corporate risk levels.
- Control-P Function represents adequate strategies to aid businesses or individuals to ensure the data with sufficient accuracy for handling privacy risks.
- Communicate-P – Develop and implement appropriate strategies to allow businesses and individuals to get a reputable comprehension and participate in an interaction regarding what data is processed and the privacy risks.
- Communicate-P Function recognises that companies and people may need to properly comprehend how data is processed to manage privacy risks.
- Protect-P – Create and implement suitable data processing safeguards to handle data protection to minimise cybersecurity-related privacy issues and conflict between privacy and cybersecurity risk management.

Categories are divided into groups of privacy results connected to organisational needs and specific activities. Subcategories within a Category are further differentiate based on the outcome of technical and administrative processes. They include findings that aim to achieve the objectives in every Category.

Profiles[222] are a component of particular Functions, Categories, and Subcategories from the Core that a business has emphasised to support it in managing privacy risk. Profiles might indicate the current status of privacy activities and the intended goal. A Current Profile highlights the privacy discoveries that businesses are actively seeking. In contrast, a Target Profile identifies the conclusions required to achieve the necessary privacy risk management objectives. The distinctions between the two Profiles enable businesses to evaluate inadequacies, develop a strategy for development, and estimate the resources needed (e.g., people, financing) to accomplish privacy results. This is the cornerstone of a business's cost-effective privacy risk-minimization approach.

Implementation Tiers[223] assist businesses in deciding how to handle privacy risks by considering the actual nature of the privacy risks posed by an organisation and the fulfilment of the methods and techniques to manage them. The Implementation Tiers can enable an

[222] Ibid, p.8;
[223] Ibid;

internal interaction about those or other aspects affecting a business's ability to handle privacy. The Privacy Framework outlines four tiers for dealing with privacy risks. Tiers define whether risk management solutions are appropriate in those various businesses. Tier 1 businesses have only adopted measures to a limited extent. Tier 2 consists of informal risk management measures that do not include a company-wide plan. Tier 3 ("Repeatable") risk management systems are entirely established and institutionalised, whereas Tier 4 ("Adaptive") businesses include new privacy problems continually.

5.5. GAPP MATURITY MODEL

Businesses acquire more personal data globally as commercial systems and methods get more complicated and advanced. As a result, personal data is subject to a variety of dangers. The Canadian Institute of Chartered Accountants and the American Institute of Certified Public Accountants collaborated to develop the Generally Accepted Privacy Principles (hereinafter "GAPP") to help businesses understand their privacy liabilities and establish an appropriate privacy program for monitoring and minimising privacy risks. The GAPP framework is based on the fundamental privacy aim, which states that personal information is collected, used, maintained, published, and handled under the entity's privacy notice obligations and the standards established in GAPP.[224]

The GAPP was designed to reflect significant local, national, and global privacy standards from a business standpoint. GAPP combines many privacy criteria into a single privacy goal backed by ten privacy principles. Each notion is supported by objective criteria that serve as the foundation for effective privacy risk and compliance management. In addition to the standards, informative policy requirements, communication techniques, and control mechanisms are offered to support them. The following are GAPP's ten principles[225]:

- *Management*: The company explains documentation, communicates with individuals and holds people accountable for its privacy policies and procedures.
- *Notice*: The company educates the public on its privacy policies and processes, as well as the goals for collecting, utilising, maintaining, and releasing personal information.

[224] AICPA and CICA (2009), Generally Accepted Privacy Principles, p6. Available at: https://bcourses.berkeley.edu/courses/1457298/files/70759534/download?verifier=k75et0haGLJqYtVlHNos0BiXVLdNOOEIjNCL2zBG&wrap=1; [Accessed on 30 January 2022];
[225] Ibid, p.7;

- *Consent and choice*: The company notifies the individual of the available options and obtains consent for PI collection, use, and disclosure.
- *Collection*: The company collects personal information solely for the purposes specified in the notice.
- *Use, retention, and disposal*: PI is only used for the reasons specified in the notice, and the subject has given consent. PI is retained for no longer than is necessary to achieve the above purposes or as legally required, and it is then correctly disposed of.
- *Access*: Individuals can access and modify their PI thru the organisation.
- *Disclosure to third parties*: Personal information is disclosed to third parties only for the purposes specified in the notice or if the individual gave their consent.
- *Security for privacy*: The company protects PI from illegal access.
- *Quality*: The company keeps accurate, comprehensive, and important PI for the reasons mentioned in the notice.
- *Monitoring and enforcement*: The company monitors adherence to its privacy policies and procedures and has systems to manage privacy issues and complaints.

Maturity models are a well-known method of comparing a company's performance to predetermined criteria. As a result, they know that growth helps the company regardless of whether it has reached all standards.

III. DIFFERENT APPROACHES TO DATA SHARING

Despite the increased demand for data and proof of its economic and social advantages, data access, sharing and re-use are still far from reaching their full potential, while they are allocated unequally on the market. Consequently, many businesses are hesitant to share their data with their competitors even though many governments recognise the benefits of open data and make public data available to the public on a broad scale.[226] Individuals, businesses, and governments frequently encounter data access restrictions, sometimes exacerbated by a reluctance to exchange data within and between sectors. On the other hand, data protection regulations have become a substantial obstacle to the cross-border share of personal data, despite open data rules requiring greater access to data. The distance between these two opposing responsibilities is becoming increasingly tight. When parties share data, they face a

[226] Phillips, M.(2018), *International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)*. *Hum Genet* 137, 575–582 (2018).p.575. Available at: https://doi.org/10.1007/s00439-018-1919-7; [Accessed on 07 January 2022];

risk of digital security and privacy breaches, as well as the infringement of other legitimate private interests (e.g.IPRs). The privacy frameworks can assist in developing privacy and security regulations for privacy and data protection that make compliance easier to achieve. However, the conditions for sharing and re-using data vary substantially among privacy standards, resulting in legislative uncertainty and a lack of openness and clarity. Therefore, new regulations to guarantee digital trade and data flows are critically required in the global digital economy.

1. OPEN DATA

As ICT advances, increased data production requires greater openness and sharing.[227] Regulation of digital products and services, cloud computing applications, the Internet of Things (hereinafter "IoT"), and artificial intelligence (hereinafter "AI") would be impossible if data flow across borders were restricted. [228] Open (Government) data is a vital public asset that provides opportunities for innovative policies and economic and social progression. Open Data can be defined as freely usable, modifiable, and shareable information by anyone for any purpose.[229] It is available under an open license that guarantees free access and the possibility for anyone to re-use it without technical, legal or financial restrictions in a machine-readable, convenient, and modifiable form.[230] Thus, data openness is comprised of two components:[231]

1. The data must be „legally" open, meaning it needs to be in the public domain or subject to liberal terms of use without restrictions.
2. The data must be „technically" open- meaning it must be disclosed in machine-readable and non-proprietary electronic formats, allowing anyone to access and use the data with standard, freely available software tools.

It is significant to mention that real-time or dynamic data should be used to achieve the best results from data openness. This type of data is most useful when it is made available for

[227] Monino, J.-L. and Sedkaoui, S. (2016) *Big data, open data and data development*. 1st edition. Hoboken, New Jersey :: ISTE Ltd/John Wiley and Sons Inc.p.xxxiii. Available at: https://onlinelibrary-wiley-com.uaccess.univie.ac.at/doi/book/10.1002/9781119285199; [Accessed on 05 January 2022];
[228] Burri, M. (2021) "*Data Flows and Global Trade Law*", Cambridge: Cambridge University Press, pp. 11–41.p.13, Available at: https://www.cambridge.org/core/books/big-data-and-global-trade-law/data-flows-and-global-trade-law/E98D121FC172A9F534DE9C310919E389; [Accessed on 05 January 2022];
[229] Available at: http://opendefinition.org/; [Accessed on 07 January 2022];
[230] European Commission, Directorate-General for the Information Society and Media, Carrara, W., Fischer, S., Steenbergen, E., et al. (2017) *Creating value through open data: a study on the impact of re-use of public data resources*. Publications Office,p.21. Available at: https://data.europa.eu/doi/10.2759/328101; [Accessed on 07 January 2022];
[231] Available at: http://opendatatoolkit.worldbank.org/en/essentials.html; [Accessed on 08 January 2022];

re-use as soon as it is collected. The Application Programming Interface (hereinafter "API") is the commonly used technology for distributing real-time data.[232] Since 2006, the European Commission (hereinafter "EC") has made its documents freely available for commercial and nonprofit usage. It was also committed to publishing documents in a machine-readable format, and to establishing an Open Data Portal to facilitate the accessibility and re-use of this data in 2011. The European Union Open Data Portal makes data stored by the European Commission and other EU institutions and bodies. The European Commission published a comprehensive open data package in 2011, examining the possibility for additional data openness, particularly data supplied by the public sector. The goal of this package was to strengthen the PSI Directive[233]. Additionally, the EU adopted the G8 Open Data Charter in June 2013 and pledged to execute a variety of open data initiatives in the G8 members' Collective Action Plan[234]. The G8 Open Data Charter acknowledges the value of open data in strengthening government and governance and encouraging economic growth via data-driven product and service innovation. It promotes the open by default, open data by default, quality and quantity, useable by all, releasing data for improved governance and innovation principles. The Open Data Directive[235] is a crucial element of the European Union legal framework regulating open data and public sector information re-use. The Directive results from an EU policy initiative that started with the first directive in 2003. The Open Data Directive aims to overcome the obstacles that continue to restrict the complete re-use of public sector information by empowering the Member States to re-use public sector data, focusing on publishing datasets with high economic and societal value. Not every country has established an open data strategy. Still, instead, it has the open data component incorporated in broader digital or open government data strategies or their open data policies. Action plans with different measures are included in the open data policy and strategy to make the open data more tangible. For example, the Federal Ministry for Digital and Economic Affairs created an "Austrian Digital Action Plan" in 2020, aiming to implement measures to enhance social and economic added value

[232] Slovenia has adopted the "Strategic Work Plan for Open Data 2020-2021" to encourage local communities to transmit real-time data via IoT sensors. Furthermore, the Law on Access to Information of Public Importance for the Implementation of the Open Data Directive requires public bodies that create or receive dynamic data to re-use it directly after collection and to enable mass transfer via API, *see* https://podatki.gov.si/sites/default/files/reports/Open%20Data_Strates%CC%8Cki%20delovni%20plan_julij2020.pdf ; [Accessed on 08 January 2022];

[233] Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, *OJ L 345, 31.12.2003, p. 90–96;*

[234] More information is avaliable at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=3489; [Accessed on 06 January 2022];

[235] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, *OJ L 172, 26.6.2019, p. 56–83;*

through effective data use, data awareness, and data transparency and traceability.[236] For personal data, the GDPR has a direct impact and requires data subjects to provide clear and explicit consent to the processing of their data.[237] However, personal data may be disclosed in the following circumstances:

- If there are, for example, public or legitimate interests to publish personal data (e.g. preventing fraud), following Article 6. of the GDPR. In general, this restricts the right to privacy;
- If the data has been anonymised. When data is anonymised, it no longer contains personal data and is exempt from the GDPR.

In comparison, in the United States, privacy and data protection are governed by sectoral laws that are less intrusive and market-based. Before 2009, the government's attempts to make data public were mainly focused on the eGovernment Act, which included the creation of a catalogue of federal public domain websites, such as websites that support a single business function or dataset (e.g., Regulations.gov 2003) and websites as a result of other laws (e.g., USASpending.gov 2007). Following the launch of the data.gov portal by the United States in 2009, there was a rapid increase in national and subnational open data portals and digital and eGovernment strategies of open governments. President of the U.S., Barack Obama, signed an Executive Order[238] mandating that all federal government information be open and machine-readable. The Office of Management and Budget issued an Open Data Policy on the same day, highlighting the significance of handling data as an asset and optimising the usability of existing datasets by making them open. Under the Open Data Policy, the agencies must make data available based on open licenses and use shared cores and extensive metadata through machine-readable and open formats. Also, agencies must build information systems to support interoperability and information accessibility. A Memorandum was issued with the Executive Order outlining how the federal government agency would implement the new open data policy. Moreover, the Digital Accountability and Transparency Act of 2014 (hereinafter "DATA Act") was enacted due to this order, which established standards for financial data to

[236] Available at: https://www.digitalaustria.gv.at/aktionsplan.html; [Accessed on 05 January 2022];
[237] Available at: https://data.europa.eu/en/datastories/protecting-data-and-opening-data; [Accessed on 05 January 2022];
[238] Available at: https://obamawhitehouse.archives.gov/the-press-office/2013/05/09/executive-order-making-open-and-machine-readable-new-default-government-; [Accessed on 05 January 2022];

optimise transparency about government spending and improve the quality of data submitted to USASpending.gov.[239]

In 2011, the Open Government Partnership was established as an international platform to improve the quality and effectiveness of public services through open data to become more transparent, accountable, and accountable to citizens. Following a global consultation led by key representatives from OGP governments, including the United Kingdom, Canada, and Mexico, civil society organisations such as the World Wide Web Foundation and Open Data Institute, and the Initiative for Latin American Open Data, the International Open Data Charter (hereinafter "ODC") was launched on the margins of the United Nations General Assembly in 2015. Based on the G8 Open Data Charter, the International Open Data Charter outlined six fundamental principles: (1) open by default; (2) timely and comprehensive; (3) accessible and usable; (4) comparable and interoperable; (5) for improved governance and citizen engagement; and (6) for inclusive development and innovation.[240] Despite these efforts to increase data openness, national and international regulations governing intellectual property rights, privacy, and personal data protection restrict open access to data.[241]

1.1. LEGAL APPROACHES TO SHARING DATA

The criteria for cross-border transfers of personal data vary widely among privacy regulations, raising regulatory complexity and ambiguity and resulting in minimal transparency and clarity of rules. There are various approaches for transferring data across borders.[242]

- Some countries allow data transfer, i.e. they lack data transfer legislation (e.g. the LDCs). This type of data transfer is known as free flow;
- The second approach, ex-post accountability, does not restrict or place special requirements on cross-border data movement (e.g. the U.S.). Nonetheless, it necessitates ex-post accountability for the data exporter if mistreated cross-border data;

[239] Ayre, L.B. and Craner, J. (2017) 'Open Data: What It Is and Why You Should Care', *Public library quarterly (New York, N.Y.)*, 36(2), pp. 173–184. Available at: https://www.tandfonline.com/doi/abs/10.1080/01616846.2017.1313045. [Accessed on 08 January 2022];
[240] Lee, Jyh-*An (2017), Licensing Open Government Data* , Hastings Business Law Journal, Vol. 13, No. 2, , The Chinese University of Hong Kong Faculty of Law Research Paper 2017-07,p.213. Available at SSRN: https://ssrn.com/abstract=2964704 [Accessed on 29 March 2022];
[241] Wessels, B. *et al.* (2017) *Open Data and the Knowledge Society*. Amsterdam: Amsterdam University Press. Available at: https://library.oapen.org/bitstream/handle/20.500.12657/31743/625332.pdf?sequence=1&isAllowed=y; [Accessed on 08 January 2022];
[242] Javier López González and Francesca Casalini (2019) *Trade and Cross-Border Data Flows*. OECD Publishing. doi:10.1787/b2023a47-en.p.17; [Accessed on 08 January 2022];

- Conditional flows on safeguards is a third approach comprising procedures that rely on evaluating sufficiency or equivalence as ex-ante requirements for data transfer (e.g. the EU). These decisions can be made by a public authority or private businesses and might include regulations for handling data. Companies can relocate data without an adequacy assessment using binding corporate rules, SCCs, etc.;
- The last broad method, flow conditional on ad hoc authorisation, refers to systems that only enable data to be sent on a case-by-case basis, subject to examination and permission by competent authorities (e.g.the PRC). This approach applies to personal data for privacy concerns and the larger scope of "important data," including information relevant to national security.

Most international data transfers require the data subject's consent, but the requirements differ by country. Numerous exceptions are provided for different types of approaches to allow data transfer. The GDPR establishes the general principle that transfers of personal data undergoing processing or intended for processing after transfer to a third country or an international organisation must comply with the GDPR.[243] The transfer of personal data to third countries must also comply with the provisions of Chapter V of the GDPR, as well as the requirements of the GDPR relating to the processing of personal data, such as limitation of purpose and liability[244], the purpose of processing[245] and personal data protection obligations[246]. Furthermore, the controller must establish that the data recipient has the right to process the personal data that will be transferred. The protection obtained by the GDPR is not put at risk by the cross-border transfer of personal data. The data controllers and processors that transfer data must assess whether the third country provides a level of protection for personal data that is equivalent to that of the EEA on an individual basis.

Transfers can be done on the basis of the European Commission's adequacy decision. According to the CJEU, "adequate" implies "essentially equivalent" to the degree of protection of fundamental rights and freedoms by the CFR and the DPD[247]. In that instance, the Commission must determine whether the third country, territory or one or more specific sectors with that third country or international organisation provide adequate protection.[248] As a result of such a decision, transfers to the country in question will be treated the same as within the

[243] Article 44 and Recital 101 of the GDPR;
[244] Article 5. of the GDPR;
[245] Article 6. in addition to Article 9. of the GDPR;
[246] Article 32. of the GDPR;
[247] See case *C 362/14 Maximillian Schrems v. Data Protection Commissioner* [2015] ECLI:EU: C:2015:650, paragraph 73;
[248] Article 45. of the GDPR;

EU data transfers. [249] Except for the UK, these adequacy decisions do not allow data transfer in law enforcement, as governed by Article 36. of the Law Enforcement Directive[250].

The EU-U.S. Privacy Shield adequacy decision, which allowed the free flow of data to companies certified in the United States, was invalidated by the CJEU in the Schrems II case[251]. Due to U.S. surveillance laws that allow the collection of EU personal information without appropriate consideration of proportionality, necessity, and redress, the CJEU declared that the EU-U.S. Privacy Shield could not provide protection equivalent to that established within the EU. Based on the Schrems II decision, the European Commission has established new SCCs, such as the requests to conduct a transfer impact assessment (hereinafter "TIA") and obligations on the entity in the third country to obtain information on government access requests where legally possible. Furthermore, on March 25, 2022, the European Commission and the U.S. had achieved an agreement "*in principle*" on a new Trans-Atlantic Data Privacy Framework, and it is necessary to formalise the details of this agreement and turn it into legal documents that will serve as the basis for the EC's draft adequacy decision. The Trans-Atlantic Data Privacy Framework will rebuild an essential legal framework for EU personal data transfers to the U.S. The U.S. has committed to implementing new safeguards to ensure that signals intelligence activities are necessary and proportionate to pursue defined national security objectives, secure the privacy of EU personal data, and create a two-level independent mechanism for EU individuals to seek redress with binding authority to direct remedial measures, as well as to enhance stringent control of signals intelligence activities to ensure compliance.[252] After the European Commission provided new SCCs based on the Schrems II judgement, the UK opted to use previous SCCs following Brexit. However, on March 21, 2022, the International Data Transfer Agreement (hereinafter „IDTA")[253] and the international data transfer Addendum (hereinafter „the Addendum") were approved by UK Parliament to replace

[249] The European Commission has so far acknowledged Andorra, Argentina, Canada (commercial organisations), the Faroe Islands, Guernsey, Israel, the Isle of Man, Japan, Jersey, New Zealand, the Republic of Korea, Switzerland, the United Kingdom under the GDPR and LED, and Uruguay provide adequate protection. The adequacy decisions for the United Kingdom include a sunset clause, meaning they run out after four years., *see* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. [Accessed on 08 January 2022];

[250] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119, 4.5.2016, p. 89–131;*

[251] See case *C-311/18 Facebook Ireland and Schrems,* ECLI:EU:C:2020:559;

[252] Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087; Accessed [29 March 2022];

[253] International Data Transfer Agreement (2022), available at: https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf; ; [Accessed on 10 April 2022];

the existing SCCs. The IDTA and the Addendum are transfer mechanisms designed to provide appropriate safeguards[254] for personal data transferred from the UK to countries that do not meet the UK's "adequacy criteria".

The Austrian Data Protection Authority (hereinafter Austrian DPA, in German *Österreichische Datenschutzbehörde*) has decided[255] in a case brought against an Austrian website provider and Google LLC by the non-governmental organisation, None of Your Business (hereinafter "NOYB") that the continued use of Google Analytics infringes the GDPR because it does not fulfil the GDPR's requirements for the safe transfer of personal data. The Austrian DPA determined that the Standard Contract Clauses ("SCCs") agreed to by the website operator and Google LLC do not provide adequate protection under the GDPR because the SCC terms were not binding on U.S. authorities. Specifically, Google LLC qualifies as an *electronic communications services provider* and is thus subject to the oversight of U.S. intelligence agencies under U.S. surveillance law, i.e. Section 702 of the Foreign Intelligence Surveillance Act of 1978. Furthermore, Google's additional safeguards have been ineffective in closing the legal gaps identified in the *Schrems II* decision. This is the first decision on the 101 model complaints filed by NOYB following the "Schrems II" judgement.

Countries that have not met the adequacy decision may use other appropriate safeguards for the cross-border transfer of personal data to compensate for the lack of data protection and establish that data subjects have enforceable rights and effective remedies. These appropriate safeguards may include legally binding and enforceable instruments between public authorities or bodies, binding corporate rules, standard data protection clauses adopted by the European Commission, standard data protection clauses adopted by a supervisory authority and approved by the European Commission, an approved code of conduct under Article 40. or an approved certification mechanism following Article 42. together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including data subjects' rights. Specific derogations to the GDPR's cross-border personal data transfer restriction allow a transfer without an adequacy decision or appropriate safeguards.[256] According to Article 49. of the GDPR derogations are exceptions to the rule that

[254] Article 46 (2) (d) of the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (S.I. 2019/419), **reg. 1(2),** Sch. 1 para. 39(3)(c) (with reg. 5); 2020 c. 1, Sch. 5 para. 1(1);

[255] R.Österreich Datenschutzbehörde, Case: D155.027 2021-0.586.25, Available at: https://privacyblogfullservice.huntonwilliamsblogs.com/wp-content/uploads/sites/28/2022/01/E-DSB-Google-Analytics_DE_bk_0.pdf; [Accessed on 10 January 2022];
This Austrian DPA's decision is not final, i.e. it is still possible to file an appeal. Moreover, according to the GDPR, the Austrian DPA's jurisdiction is typically restricted to Austria.

[256] Article 49 (1)of the GDPR;

personal data may only be transferred to third countries if the third country provides adequate protection or safeguards. Data subjects have enforceable and effective rights to continue to benefit from their fundamental rights and safeguards[257]. Moreover, a derogation is available when the data subject has given explicit informed consent to the transfer.[258] Alternatively, a derogation may apply if the transfer is necessary for the performance of a contract between the data subject and the controller,[259] conclusion or performance of a contract concluded in the data subject's interest,[260] for important reasons of public interest[261], for the establishment, exercise, or defence of legal claims[262], to protect the vital interests of the data subject or other persons[263], and if the transfer is made from a register that, according to Union or Member State law, is intended to provide information to the public and is open to consultation by the general public or by anyone who can demonstrate a legitimate interest.[264] Hence , there are some ground rules to follow when it comes to derogations. This is primarily reflected in the fact that derogations are of a subsidiary nature, while they can be applied if there is no adequacy decision or adequate safeguards. Derogations apply to non-repetitive activities involving a limited number of data subjects. They must be necessary for the controller's legitimate interests, which do not override the subject's interests, rights, or freedoms. Moreover, the controller needs to implement adequate safeguards for personal data protection, notify the supervisory authority, and inform the data subject of the transfer and the relevant legitimate interests.

However, data sharing and re-use are very important factors to consider in the data economy, even though private and personal data provide distinct barriers to the free flow of data.[265] The Regulation on the Framework for the Free Movement of Non-Personal Data Across Borders[266] was introduced to remove barriers to the free movement of non-personal data and make it more accessible to switch data storage and processing providers. This type of Regulation supplements the GDPR framework, which covers personal data and aims to remove

[257] EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0;
[258] Article 49 (1)(a) of the GDPR;
[259] Article 49 (1)(b) of the GDPR;
[260] Article 49 (1)(c) of the GDPR;
[261] Article 49 (1)(d) of the GDPR;
[262] Article 49 (1)(e) of the GDPR;
[263] Article 49 (1) (f) of the GDPR;
[264] Article 49 (1)(g) of the GDPR;
[265] Curry, Zillner, S., Metzger, A., Pazzaglia, J.-C., & Robles, A. G. (2021). *The Elements of Big Data Value: Foundations of the Research and Innovation Ecosystem*. National University of Ireland, p.52 – 56; Available at: https://link.springer.com/book/10.1007/978-3-030-68176-0; [accessed 27 January 2022];
[266] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union PE/53/2018/REV/1 *OJ L 303, 28.11.2018, p. 59–68;*

barriers to the free movement of non-personal data between EU countries. Understanding the significance of monitoring data flows to inform EU decision-making and investment choices in cloud computing, the European Commission issued a Communication on a European Strategy for data[267] in 2020 to create a "European analytical framework for measuring data flows".[268] The proposed Data Governance Act also outlines rules for international transfers of protected public sector data. The main goal of harmonising data protection laws within the EU is to create a single European market for processing personal data in which member states will not restrict or prohibit the free movement of personal data between member states.

Furthermore, Industrial Data Platforms (hereinafter "IDPs") and Personal Data Platforms (hereinafter "PDPs") are two theoretical solutions that have the potential to reduce current barriers to unrestricted data flow significantly. IDPs have been recognised as potential drivers for increasing the European Data Economy in response to the expansion of data markets, focusing on the necessity to offer robust and secure data transfers, notably in the business sector.[269] The IDP solution is intended for private data, and its application should enable a safe and legal environment. European Innovation Spaces (or i-Spaces) are the ideal way to analyse IDP since they serve as a platform for combining technical and non-technical activities, including merging technology and application development and nurturing skills, competencies, and best practices. The concept of PDP has emerged as a possible solution that might enable data subjects and owners to preserve control over their data and its further use. For personal data storage and access, PDPs use the concept of user-controlled cloud-based technology. However, consumers have only been able to maintain and restrict access to a limited collection of personal data thus far since they have connected their social media profiles to several growing Personal Information Management Systems (hereinafter "PIMS")[270].

In the United States there are no data transfer restrictions**.** Moreover, the CCPA includes particular provisions regarding data transfer resulting from mergers and acquisitions, allowing consumers to opt-out of the third uses of personal information in a manner that is significantly inconsistent with "*the promises made at the time of collection*".[271] Without a Mutual Legal

[267] EC (2020), Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, A European strategy for data, *COM(2020)66 final*, Brussels;
[268] Ibid;
[269] Curry, Zillner, S., Metzger, A., Pazzaglia, J.-C., & Robles, A. G. (2021). *The Elements of Big Data Value: Foundations of the Research and Innovation Ecosystem*,(n 265);
[270] Ibid;
[271] CCPA Section 1798.140. (C);

Assistance Treaty (hereinafter "MLAT"), the CLOUD Act[272] permits court orders or warrants demanding the transfer of personal information. The EDPB[273], on the other hand, determined that service providers under EU regulations cannot lawfully act on such demands to disclose and transfer personal data to the United States. According to GDPR, court orders mandating data transfer beyond the EU are only valid if they have been based on an international agreement, such as an MLAT.[274] Other legal justifications for comparable demands are prohibited by EU legislation.

The People's Republic of China's cyber security and data legislation, such as the Data Security Law (hereinafter "DSL") and the PIPL, set restrictions on cross-border data transfers and, in certain situations, need governmental security evaluations. Under the PIPL, when a personal information processor is required to transfer personal information due to a merger, division, dissolution, or being declared bankrupt, the individual must be notified of the recipient's name and contact information. The recipient must carry out its obligations as a personal information processor. The recipient must fulfil its responsibilities as a personal information processor. If the initial purpose and processing method are altered, the recipient must seek the individual's agreement again in line with PIPL.[275]

Personal data processors who wish to transfer personal data outside the PRC must obtain separate consent from the relevant individual. Furthermore, data processors must meet the following requirements: passing a security assessment under Article 40. conducted by the PRC cyberspace administration, obtaining a personal information protection certification issued by a PRC cyberspace administration accredited institution, entering into standard contracts formulated by the PRC cyberspace administration, or other conditions specified in the laws and administrative regulations of the PRC cyberspace administration. Furthermore, the PI processor must guarantee that the overseas recipient's processing operations comply with the personal information protection standards outlined in e the PIPL.[276]

[272] Clarifying Lawful Overseas Use of Data or CLOUD Act 18 U.S.C. §§2323,2713 (2018);
[273] EDPB (2019), *ANNEX. Initial legal assessment of the impact of the U.S. CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-U.S. Agreement on cross-border access to electronic evidence,p.3* Brussels. Available at: https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf; [Accessed on 13 January 2022];
[274] Article 48. of the GDPR;
[275] Article 22. of the PIPL;
[276] Article 38. of the PIPL;

Before transferring PI outside of the PRC, all personal information processors must conduct an internal personal information protection impact assessment[277], which needs to examine:[278]

- whether the purpose and method of the outbound transfer of PI is legal, justified, and necessary;
- the impact on individuals' rights and interests, as well as security threats;
- whether the safeguard measures are legal, effective, and adequate for the risk levels.

Different types of data have various cross-border export limitations under the DSL. The DSL mandates that controlled item data be subject to export control restrictions.[279] Important data collected and processed by CIIOs in the PRC comply with the Cybersecurity Law regarding cross-border transfers, whereas other important data collected and processed by other data operators in the PRC to be transferred cross-border are regulated by the State internet information department in collaboration with the relevant State Council departments.[280] The DSL[281] and PIPL[282] generally forbid the transfer of data and personal information kept in the PRC to a foreign judicial or enforcement authority without prior consent from the PRC competent authority. However, data transfer is possible if relevant laws and international treaties and agreements are adopted, signed or participated in by the PRC.

Regarding the transfer of personal data from Bosnia and Herzegovina to another state or international organisation if adequate protection measures as defined in the Law on Personal Data Protection have been implemented. Personal data may be transferred from Bosnia and Herzegovina to another state that does not provide adequate protection measures when the disclosure of personal data is required by law or international agreement, when the data subject has given prior consent, and when it is necessary to disclose personal data for the performance of a contract between Bosnia and Herzegovina and another state, and provided that such transfer is needed to meet legal claims, to save lives and vital interests of data subjects, and to protect public interest[283].

[277] Article 55. of the PIPL;
[278] Article 56. of the PIPL;
[279] Article 25. of the DSL;
[280] Article 31. of the DSL;
[281] Article 36. of the DSL;
[282] Article 41. of the PIPL;
[283] Article 18 of the LPDP of Bosnia and Herzegovina;

1.1.1. BILATERAL AND PLURILATERAL AGREEMENTS

Businesses and individuals do not have to rely on government authorities to eliminate restrictions on their data flow since they may do it themselves using various strategies such as agreements, contracts, waivers and licenses.

Even though the General Agreements on Trade in Services (hereinafter "GATS")[284] does not directly regulate cross-border data flows, such flows may be covered by cross-border trade when data transfers promote the supply of services across borders. The WTO Members formed the Work Programme on Electronic Commerce in 1998 to evaluate all trade-related problems related to global electronic commerce, but this was not designed as a formal negotiation platform.[285] Since then, WTO Members have neglected to renew their service obligations under GATS, restricting its relevance to digital trade challenges. However, in response to technological advances, new international legal standards for digital trade have been evolving through bilateral and plurilateral trade agreements.

The free trade agreements (hereinafter "FTA") frequently require parties to provide unrestricted cross-border data flows, including personal data. The autonomy of states in maintaining and implementing measures through the FTA to promote national policy objectives is sometimes called the right to regulate. According to the WTO Appellate Body, the right to regulate in international trade law includes the ability to regulate in response to trade liberalisation commitments and the ability to regulate in opposition to such obligations.[286] Most provisions are found in the e-commerce and intellectual property chapters but can also range from customs taxes and paperless trading to personal data protection and cybersecurity. Despite widespread discourse and extensive use, there is no consensus on a definition of data flows in FTAs. Most FTA includes an exception that allows parties to diverge from it to impose and sustain regulation in the public interest.[287] The scope of FTA digital trade covering has also increased over the years. Older agreements were more likely to include only a few clauses on e-commerce, while today's FTA became more complicated with coverage of several policy

---

[284] General Agreement on Trade in Services (1994), Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167;

[285] Soprana, M.(2021). *The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block*. Trade, Law and Development. XIII. 143.p.147. Available at: https://www.researchgate.net/publication/354472706_The_Digital_Economy_Partnership_Agreement_DEPA_Assessing_the_Significance_of_the_New_Trade_Agreement_on_the_Block; [Accessed on 16 January 2022];

[286] Yakovleva, S. (2018) "*Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?*," (n 19);

[287] HODSON, S. (2019) "*Applying WTO and FTA Disciplines to Data Localization Measures,*" World Trade Review. Cambridge University Press, 18(4), pp. 579–607, P.597. Available at: https://doi.org/10.1017/S1474745618000277; [Accessed on 12 January 2022];

areas. The first FTA to incorporate an e-commerce clause, paperless trading, was inked in 2000 by New Zealand and Singapore[288], while Jordan and the United States[289] signed the first bilateral FTA that includes an e-commerce section. Since then, agreements with particular provisions or chapters on e-commerce and digital trade have increased significantly. On February 17, 2003, the Australia–Singapore FTA[290] became the first FTA to contain a particular chapter on e-commerce. The EU-Japan EPA[291] addressed e-commerce and digital trade concerns as part of broader trade discussions that included IPRs, technical trade barriers, services, and rules of origin[292].

The FTAs expressly incorporate personal data in data-related terms, exposing potential issues with domestic data protection legislation. Personal data protection in these FTAs varies and may include a comprehensive spectrum of binding and non-binding regulations, symptomatic of the underlying tensions between the regulation purposes of innovation and data protection. The Jordan–U.S. FTA Joint Statement on Electronic Commerce states that adequate privacy protection is required to process personal data on global information networks. Nevertheless, it also says that privacy protection methods should be flexible, that parties should motivate the private sector to design and implement enforcement mechanisms, and that the OECD Privacy Guidelines provide an appropriate basis for policy development. The EU and Japan EPA did not specify how they intended to regulate cross-border data flows, instead of committing to evaluating the necessity for free flow data provisions in their agreement within three years[293]. Some FTAs require that when developing online personal data protection standards, each party consider existing international standards (e.g., Argentina–Chile FTA[294]) as well as standards or guidelines of relevant international organisations (e.g., Australia–China

[288] Closer Economic Partnership Agreement between New Zealand and Singapore (2000), and upgraded in 2020 Available at: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/nz-singapore-closer-economic-partnership/cep-text/#bookmark1 ; [Accessed on 16 January 2022];
[289] U.S. – Jordan Free Trade Agreement (2001). Available at: https://ustr.gov/trade-agreements/free-trade-agreements/jordan-fta/final-text; [Accessed on 20 January 2022];
[290] The Singapore-Australia Free Trade Agreement (2003), and upgraded in 2021. Available at: https://www.dfat.gov.au/sites/default/files/agreement-to-amend-the-singapore-australia-free-trade-agreement.pdf; [Accessed on 20 January 2022];
[291] Agreement for an Economic Partnership, EU-Japan, 2018 O.J. (L 330). Available at. http://publications.europa.eu/resource/cellar/d40c8f20-09a4-11e9-81b4-01aa75ed71a1.0006.01/DOC_1; [Accessed on 20 January 2022];
[292] Soprana, M.(2021). *The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block*. (n 285), p.147;
[293] Ibid, p.156;
[294] Argentina - Chile FTA (2017). Available at: https://edit.wti.org/document/show/bf9aa665-cb2a-472f-849d-090e28b096fb?textBlockId=834843bf-fbff-4d65-8829-67b41e122cf7&page=15; [Accessed on 17 January 2022];

FTA[295]), such as the APEC Privacy Framework and the 2013 OECD Guidelines on Transborder Flows of Personal Data, or provide a high level of protection compatible with the international standards (e.g. Armenia–EU CEPA[296]).[297]

Several FTAs place a specific focus on the transfer of personal data, mandating it only if required for the competent authorities to execute agreements signed between the parties (e.g. EC–Moldova AA) or that the nations have a sufficient degree of safeguards for the protection of personal data (e.g. Korea–Vietnam FTA[298]). Some FTAs provide that the parties will support the use of encryption or security procedures for users' personal information, as well as its dissociation or anonymisation, when such data is transmitted to third parties (e.g. Brazil–Chile FTA[299])[300]. The FTAs, primarily initiated by the EU, include chapters on personal data protection, such as the principles of purpose limitation, transparency, security, right to access, rectification, and opposition, transfer restrictions, sensitive data protection, and enforcement mechanisms[301]. The United States-Korea Free Trade Agreement (hereinafter "KORUS FTA")[302] is a commonly used legal mechanism regulating data transfer. The KORUS FTA was one of the first to underline the value of free information flow in enabling commerce, recognising the need for personal information protection, and restricting unnecessary obstacles to cross-border information flows. Despite its repeated use of the term, there is no common understanding of a definition of data flows in FTAs.

The European Commission and the United States have agreed in principle on a new Trans-Atlantic Data Privacy Framework, which will promote trans-Atlantic data flows and address concerns made by the CJEU in its Schrems II ruling in July 2020[303].

Many *plurilateral agreements* aim to foster cross-border data flows and build consensus on privacy principles among participating countries. There are many different

---

[295] The PRC – Australia Free Trade Agreement (2015). Available at: https://www.dfat.gov.au/trade/agreements/in-force/chafta/Pages/australia-china-fta; [Accessed on 17 January 2022];

[296] EU-Armenia Comprehensive and Enhanced Partnership Agreement (2021). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22018A0126(01); [Accessed on 17 January 2022];

[297] Burri, M. (2021) "*Data Flows and Global Trade Law*,", (n 228), p.31;

298 FTA between the Government of the Republic of Korea and the Government of the Socialist Republic of Viet Nam (2015). Available at: https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/3582/download; [Accessed on 17 January 2022];

[299] Brazil - Chile FTA (2018). Available at: https://edit.wti.org/document/show/e62cfb4c-abbf-43d9-ae34-a15c7d057ab4; [Accessed on 17 January 2022];

[300] Ibid, p.31;

[301] Ibid, p.32;

[302] United States-Korea Free Trade Agreement (2012); Available at: https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text; [Accessed on 19 January 2022];

[303] More information is available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087; [Accessed on 29 March 2022];

approaches, each with varying levels of enforceability and implications for the privacy of individuals. Non-binding plurilateral agreements rely on "soft law" to urge parties to implement data protection standards and build interoperability between privacy protection regimes to transfer data.

The *OECD Privacy Guidelines*[304] from 1980 were the first internationally recognised set of privacy principles governing personal data protection in public and private sectors. Countries are still attempting to implement them, impacting privacy law progress. Using a risk-based approach, the OECD Privacy Guidelines[305], revised in 2013, subordinated regulation of cross-border transfers of personal data to economic aspects to minimise restrictions to a minimum. The 2013 OECD Privacy Guidelines framework is based on the accountability principle, which states that a data controller is accountable for personal data under its control, irrespective of where the data is located. Therefore, the Guidelines require a Member State not to prohibit the cross-border movement of personal data if other countries follow adequate measures to provide the Guidelines or a degree of protection established under the Guidelines. Members began the process of reviewing and updating the guidelines again in 2019.

The Association of Southeast Asian Nations (hereinafter "ASEAN") accepted the ASEAN Framework on Digital Data Governance in 2018. Members of ASEAN can embrace a nonbinding plurilateral approach to digital data governance. Among the principles are encouraging cross-border data flows among and between the Member States and defining comprehensive rules for data transfer from one Member State to another. ASEAN has codified several contractual provisions (MCCs). ECOWAS and the Organisation of Ibero-American States have also established guidelines with the Supplementary Act on Personal Data Protection of 2010 and the Standards for Personal Data Protection for the Ibero-American States of 2017.

There are also plurilateral binding arrangements with enforcement mechanisms, such as *Convention No.108*. This legally binding Convention protects individuals' right to privacy in the context of the automatic processing of personal data.

The *APEC Cross-Border Privacy Rules (CBPR) System* has a binding component, although it acts differently. The CBPR System is a government-backed data privacy certification system. Businesses may join to fully comply with recognised privacy protection

[304] OECD (1980), *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris. (n.211);
[305] OECD(2013), "Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (n 212);

principles and enforcement techniques, allowing them to transfer data with more assurance across CBPR member economies. The 2005 APEC Privacy Framework and its recently amended 2015 version also consider personal data protection a potentially harmful restraint on cross-border data flows. This Framework monitors cross-border transfers of personal data based on a broad concept of accountability. Still, it does not expressly allow limitations on cross-border transfers of personal data to jurisdictions with poor personal data protection. Instead, it holds the original data collector accountable for complying with the initial data protection framework, regardless of which firms or locations the personal data is later transferred to.

The *2018 G-20 Digital Economy Ministerial Declaration*[306] identified principles to facilitate an inclusive and whole-of-government approach to the use of information and communication technology (hereinafter "ICT") and assist governments in restructuring their strategies while recognising the relevant frameworks of different countries, including privacy and data protection[307]. During its hosting year in 2019, Japan focused on data governance. The G20 Osaka Leaders' Declaration[308] acknowledged the significance of cross-border data flows but highlighted the challenges associated with data security and privacy and advocated interoperability between multiple frameworks to enable "*data free flow with confidence*" and improve the digital economy.

One of the most prominent plurilateral agreements is the *Comprehensive and Progressive Agreement for the Trans-Pacific Partnership* (hereafter "CPTPP"), which presented an innovative strategy for resolving data localisation concerns. The CPTPP is a free trade agreement signed by eleven Asia-Pacific[309] nations and contains binding measures restricting data localisation and requirements on cross-border data flow.[310] Cross-border transfer of information, including personal information, is permitted where the action is to conduct a covered person's business.[311] The legislative mechanisms used by the CPTPP Parties to protect personal data may differ. Each Party must encourage the creation of procedures to promote interoperability across these diverse regimes. These methods may include autonomous or mutual recognition of regulatory outcomes and broader international frameworks. To that

[306] G-20 Digital Economy Ministerial Declaration, "G-20 Digital Economy,", Available at: http://www.g20.utoronto.ca/2018/2018-08-24-digital.html; [Accessed on 18 January 2022];
[307] Ibid, Annexe paper 1;
[308] G-20 Osaka Leaders' Declaration (2019), Available at: http://www.g20.utoronto.ca/2019/2019-g20-osaka-leaders-declaration.html; [Accessed on 18 January 2022];
[309] The CPTPP is signed by Australia, Brunei Darussalam, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam, and the United Kingdom applied to join in February 2021.
[310] Article 14.2:1 of the CPTPP;
[311] Article 14.11 of the CPTPP;

end, the Parties shall try to convey information on such mechanisms in operation in their respective jurisdictions and investigate measures to extend these or other suitable arrangements to encourage compatibility.[312] The CPTPP's data localisation and transfer provisions are excluded from activities to accomplish a legitimate public policy aim. This exception clarifies that the CPTPP data rules do not prevent a CPTPP Party from incorporating or maintaining inconsistent measures to pursue a legitimate public policy objective, given that such actions do not constitute arbitrary or unjustifiable discrimination or a disguised trade restriction or impose more restrictions on information transfers than are necessary to achieve the objective.[313] These non-discriminatory measures are comparable to the test established in GATS Article XIV. and GATT Article XX., which aims to balance trade and non-trade interests. The CPTPP does not contain the GATT and GATS list of public policy objectives but instead refers to legitimate public policy objectives. This strengthens the regulatory authority of CPTPP signatories.[314] According to the CPTPP, it may not compel the transfer or access to the source code of software owned by another party as a condition of importing, distributing, selling, or utilising such software or goods incorporating such software in its territory. The prohibition only applies to mass-market software or goods that contain such software. Every CPTPP member must develop or maintain a legal framework that protects the personal information of e-commerce users. Still, no criteria or requirements for the legal framework have been provided.[315] The CPTPP also has a national security exemption that differs from the GATS national security exception in Article XIV. The CPTPP data standards cannot be construed to compel a Party to disclose information that is harmful to its security interests or to prevent a Party from taking steps that it believes are required to safeguard its security interests.[316]

The United States, Mexico, and Canada Agreement (hereinafter „USMCA“)[317] is the first U.S. trade agreement regarding privacy, cross-border data flows, and security provisions. The USMCA includes a chapter on Digital Trade that mirrors the CPTPP in maintaining free data flows through data localisation restrictions, nondiscrimination treatment for digital products, and a strict requirement on free information flows.[318] The USMCA recognises the economic and social advantages of protecting digital trade users' personal information and

[312] Article 14.8 of the CPTPP;
[313] Article 14.13 of the CPTPP;
[314] Burri, M. (2021) "*Data Flows and Global Trade Law*," (n 228), p.35;
[315] Article 14.18:2 of the CPTPP;
[316] Article 29.2 of the CPTPP;
[317] Government of Canada (2020) Agreement between Canada, U.S. and Mexico, Available at: https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/index.aspx?lang=eng; [Accessed on 18 January 2022];
[318] Burri, M. (2021) "*Data Flows and Global Trade Law*,", (n 228), p.37;

influencing consumer trust in digital commerce.[319] The agreement clearly emphasises that the parties may use different legal approaches to protect personal data while considering the principles and guidelines of relevant international bodies, such as the APEC Privacy Framework and the 2013 OECD Privacy Guidelines.[320] The exception clause states that parties may implement or maintain a measure incompatible with the free flow of data provision if it is necessary to achieve a legitimate public policy objective (e.g. privacy, national security), given in a way that does not create arbitrary or unjustifiable discrimination or a hidden restriction on trade, and that it does not impose restrictions on information transfers that are greater than are necessary to achieve the objective.[321] In terms of open government data, it is noted that making government data more accessible and usable to the public promotes economic and social growth, competitiveness, and innovation.[322] Furthermore, government information must be in a machine-readable and open format that can be searched, accessed, utilised, reused, and redistributed.[323] Cooperation is required to improve and produce economic prospects by extending access to and using government information, including data which is made public.[324]

The *Digital Economy Partnership Agreement (hereinafter „DEPA")*[325] was signed by Singapore, New Zealand, and Chile in January 2020. The agreement is an open plurilateral agreement[326], implying that additional countries can join it while offering the option of withdrawal.[327] South Korea, China and Canada have made official requests to enter this Agreement. This Agreement has three core objectives: enabling efficient digital trade, secure data transfers, and developing confidence in digital systems. The DEPA, like the USMCA and CPTPP, requires each Party to establish or maintain a legislative framework that protects the personal information of electronic commerce and digital trade users and to consider the principles and guidance of relevant international organisations in developing its legislative framework for the protection of personal information.[328] According to the DEPA, the core principles for a solid legislative framework for personal information protection are collection limitation, data quality, purpose definition, use limitation, security protections, transparency,

[319] Article 19.8:1 of the USMCA;
[320] Article 19.8:2 of the USMCA;
[321] Article 19.11:2 of the USMCA;
[322] Article 19.18:1 of the USMCA;
[323] Article 19.18:2 of the USMCA;
[324] Article 19.18:3 of the USMCA;
[325] Digital Economy Partnership Agreement (2020) Available at: https://www.mfat.govt.nz/assets/Trade-agreements/DEPA/DEPA-Signing-Text-11-June-2020-GMT-v3.pdf ; [Accessed on 18 January 2022];
[326] Article 16.4 of the DEPA;
[327] Article 16.5 of the DEPA;
[328] Article 4.2:2 of the DEPA;

individual engagement, and accountability.[329] It should be highlighted that the parties confirm their level of commitment in terms of cross-border data transfers[330] and computing facility placement.[331] The agreement also emphasises the need to protect consumers from fraudulent, misleading, and deceptive corporate practices. The DEPA has the most comprehensive rules on this issue, demanding that the items and services given be of acceptable and sufficient quality and that consumers receive proper recourse when they are not.[332] The DEPA includes a module devoted to new trends and technologies, concentrating on financial technology (FinTech)[333], artificial intelligence[334], government procurement[335] and digital market competition legislation[336]. All of this is done to promote the usage of AI Governance Frameworks while considering globally accepted concepts or standards such as explainability, transparency, fairness, and human-centred values.

1.1.2. LICENSE

A data license is a legal instrument that establishes standard terms and conditions for sharing and reusing data. Several standard licenses may be used to achieve open data, while bespoke licenses facilitate more data access and re-use. The usage of standard licensing can improve data interoperability and lead to increased compliance.

The Creative Commons licenses [337] (hereinafter "CC") allow unrestricted reproduction, re-use, sharing, and, in some instances, altering the original creator's creative work. Because the rights holder authorises specific permissions in advance or gives consent, there is no need to require approval from the rights holder each time. Different types of this standard licenses are established by combining attribution BY, which requires the original creator of the work to be identified, with three other essential elements[338]:

[329] Ibid;
[330] Article 4.3 of the DEPA;
[331] Article 4.4 of the DEPA;
[332] Article 6. of the DEPA;
[333] Article 8.1 of the DEPA;
[334] Article 8.2 of the DEPA;
[335] Article 8.3 of the DEPA;
[336] Article 8.4 of the DEPA;
[337] Available at: https://creativecommons.org/; [Accessed on 23 January 2022];
[338] Korn N.(2010), *Overview of the 'Openness' of Licences to Provide Access to Materials, Data, Databases and Media,* JISC Legal, p. 2. Available at: http://sca.jiscinvolve.org/wp/files/2010/12/SCA_BP_Open_Licences_Dec10_v1-02.pdf; [Accessed on 23 January 2022];

- *the non-Commercial element,* which implies the work must be used for non-commercial purposes only;
- *the non-derivatives element* represents the fact that the original work will not be modified or combined with other works, and
- *the share-alike element* means that work may be adapted, but if made accessible to the public, it must be licensed under the same conditions as the original work.

CC licenses come in six different varieties, including Attribution (CC BY), Attribution Non-Commercial (CC BY-NC), Attribution Attribution No Derivatives (CC BY-ND), Share Alike (CC BY-SA), Attribution Non-Commercial No Derivatives (CC BY-NC-ND), and Attribution Non-Commercial Share Alike (CC BY-NC-SA).

The CC Zero (hereinafter "CC0")[339] is a Creative Commons tool that simplifies transferring data, datasets, and databases into the public domain for copyright holders. If this isn't possible, a CC0 license permits the owner of the rights to provide anybody with an unlimited, royalty-free, and unconditional license to use the resource for any purpose. Any copyrights and related or adjacent rights you may have in all countries worldwide, such as moral rights, publicity or privacy rights, and rights protecting you from unfair competition, can be waived using CC0.

Open Data Commons[340] is a collection of legal tools and licenses that can assist in publishing, sharing, and using open data. The Open Data Commons is an initiative that began in 2007. Its initial license was a Public Domain Dedication License compatible with CC0. In 2009, the project was handed to the Open Knowledge Foundation, which now provides two additional licenses comparable to the Creative Commons licenses but tailored to databases, i.e. Open Data Commons Attribution License compatible with CC BY and Open DataBase License[341] compatible with CC BY SA.

The Open Government License[342] is a part of the UK Government Licensing Framework, intended for use with UK government and public sector resources, emphasising datasets, source code, and collected or original data. This license requires attribution, although modified works and commercial use are authorised, and there is no copyleft requirement. It

[339]Available at: https://creativecommons.org/choose/zero/; [Accessed on 23 January 2022];
[340] Available at: https://opendatacommons.org/; [Accessed on 23 January 2022];
[341] Available at: https://opendatacommons.org/licenses/odbl/summary/; [Accessed on 23 January 2022];
[342] Available at: https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/; [Accessed on 23 January 2022];

prohibits copying logos, registered trademarks, and other IPRs and also includes non-endorsement restrictions.[343]

1.1.3. WAIVERS

A waiver is a legal declaration by the rightsholder that no IPRs in the data set or other work protected by copyright, or sui generis database rights, will be enforced. This is the best consequence of the data set's openness since it provides full interchange with no limits other than the law[344]. However, waivers are not applicable in all jurisdictions. In the EU, GDPR rights cannot be waived, although obtaining users' consent is one method of collecting, processing, or using their data[345]. Furthermore, data protection is an integral component of the right to privacy under the ECHR. As a result, it is challenging to waive, and the present data protection regulations limit the scope of permissible contractual or property rights. The preservation of a fundamental right substantially impacts data protection, and excluding data protection from the range of privacy rights is not desirable. First, according to ECHR case law[346], privacy protection is beyond the negative right against state involvement to encompass affirmative requirements of a state to establish a data protection system. If data protection is acknowledged as anything other than a fundamental right under Article 8. of the ECHR, this will remove the restrictions imposed by the fundamental rights classification and enable complete waiver, paving the way for a significant shift in data protection policy.[347]

Even the CCPA states that any condition of a contract or agreement of any kind that purports to waive or restrict a consumer's rights under the CCPA in any way, including, but not limited to, any right to a remedy or method of enforcement, is invalid and unenforceable[348]. Despite the wording in the CCPA, the California Supreme Court held in the case of *Sanchez v. Valencia Holding Co*[349], that class action waiver provisions inside contracts are valid even if a

[343] Korn N.(2010), *Overview of the 'Openness' of Licences to Provide Access to Materials, Data, Databases and Media,* JISC Legal, (n 338), p.4;
[344] Doldirina, C., Eisenstadt, A., Onsrud, H., & Uhlir, P. (2018). *Legal Approaches for Open Access to Research Data*, p. 31. Available at: https://doi.org/10.31228/osf.io/n7gfa; [Accessed on 21 January 2022];
[345] National Research Council 2012. *For Attribution: Developing Data Attribution and Citation Practices and Standards: Summary of an International Workshop*. Washington, DC: The National Academies Press.p.74 Available at: https://doi.org/10.17226/13564. [Accessed on 21 January 2022];
[346] See the case of *I. v. Finland* ECHR (17 July 2008), application no. 20511/03;
[347] Purtova, N. (2010) '*Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights'*, Netherlands quarterly of human rights, 28(2), pp. 179–198.p.16. Available at: https://www.researchgate.net/publication/228147350_Private_Law_Solutions_in_European_Data_Protection_Relationship_to_Privacy_and_Waiver_of_Data_Protection_Rights; [Accessed on 23 January 2022];
[348] CA Civ Code § 1798.192 (2018);
[349] *See* the case of *Sanchez v. Valencia Holding Co*., 61 Cal. 4th 899 (2015);

state statute seems to allow for class action type remedies. Consequently, based on this decision, there is a compelling case to be made that the CCPA will not be understood as prohibiting consumers from deciding to waive their ability to proceed in class actions.

2. DATA PORTABILITY

Data portability is a broad term that covers a natural or legal person's ability or right to request that a data holder transfer data regarding that person, to that person or a specified third party, on a temporary or regular basis in a structured, frequently used, and machine-readable format. A structured form allows the software to extract set and well-known data pieces. A machine-readable data format can be read and processed automatically by a computer, such as Extensible Markup Language (XML) or JavaScript Object Notation (JSON).[350] The scope of data to be shared shapes data portability systems, which will usually be limited to data relevant to the user. Data portability requirements in the context of privacy law could be confined to personal data.[351] The data portability will only be helpful if other service providers can use it. This is governed by the data's structure, format, and underlying principles. Well-organised data in a transparent form, which will allow their easy transfer, could be beneficial for service providers.[352] Aside from the scope and type of data, assessing how data is transferred through a portability system is important. This includes whether data is shared once and requires additional user input or if a continuous stream of data is established. A one-time basis approach may be associated with the *right to be forgotten*[353] under privacy legislation in certain jurisdictions. Continuous data transfering, on the other hand, would demand some interoperability between the sending and receiving systems.[354]

The GDPR introduced the first broad right to data portability[355] to give more control to data subjects over their data.[356] Because it allows the direct transfer of personal data from one

[350] Wong J., Henderson T. (2019), *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, *International Data Privacy Law*, Volume 9, Issue 3, Pages 173–191, p.8. Available at: https://doi.org/10.1093/idpl/ipz008; [Accessed on 25 January 2022];
[351] OECD (2021), Data Portability, Interoperability and Digital Platform Competition, OECD Publishing, Paris, p. 10. Available at: https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf; [Accessed on 21 January 2022];
[352] Ibid, p.11;
[353] See Case C-131/12, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*, ECLI:EU:C:2014:317;
[354] Ibid;
[355] Article 20. of the GDPR;
[356] Article 29 Working Party (2017), " Guidelines on the right to data portability", WP 242 rev.01, p.4 Available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=44099; [Accessed on 21 January 2022];

data controller to another, the right to data portability is a crucial tool that will facilitate the free flow of personal data in the EU and drive competition between controllers.[357] A data subject's right to receive a set of personal data processed by a data controller about that data subject and to hold that data for future personal use is referred to as data portability. In this way, data portability supports the right of access. However, data portability distinguishes itself by allowing data subjects to manage and re-use their personal data easily.[358] Secondly, data subjects can transfer personal data freely from one data controller to another.[359] When a data subject uses the right to data portability, they do so without regard to any other right.[360] Processing operations must be based on the consent, contract or carried out by automated means to fall inside the scope of data portability.[361] However, it does not apply when a data controller executes its public obligations or complies with a legal duty.[362] To fall under the scope of the right to data portability, data must be about the data subject[363], and data that the data subject has provided to a data controller.[364] As such, GDPR is limited to provided/volunteered and observed data.[365] This right is envisaged to encourage opportunities for innovation and safe and secure transfer of personal data between data controllers under the data subject's control[366]. Additionally, the EU's Free Flow of Data Regulation aims to remove legal barriers to the portability of non-personal data, underlining that competitiveness concerns produced by lack of data portability can be caused not only by business conduct and projects but also by legal requirements. Other countries based on the EU model have similar terminology in their data portability legislation. For example, the CCPA provides that in response to a request for disclosure, a business must give personal information in a freely usable format that allows a consumer to transfer the information without interference from one entity to another[367]. Singapore, Brazil, Argentina and Mexico are among the countries that have enacted similar data portability regulations.

[357] Ibid, p.3;
[358] Ibid, p.4;
[359] Article 21 (1). of the GDPR;
[360] Article 21(3). of the GDPR;
[361] Article 21 (1)(a). and (b). of the GDPR;
[362] Article 20(3). and Recital 68. of the GDPR;
[363] Data that is anonymous or does not relate to the data subject is excluded.
[364] Article 21(1) of the GDPR;
[365] Working Party (2017), " Guidelines on the right to data portability", (n 356), p.10;
[366] Ibid, p.4;
[367] CCPA Section 1798.100(d) and 1798.130(a)(2);

The usage of APIs and compatible platforms enhance the value of data portability since they allow the transfer of useable, real-time data that recipient businesses can use.[368] The Data Transfer Project, Fair&Smart, OpenDSR, My Data Done Right, and other solutions may help ease the process of exercising the right to data portability. The Data Transfer Project tries to establish standards APIs, interoperable platforms, and other infrastructure to create an open-source, service-to-service data portability platform that allows data transfer across all businesses to be technically viable.[369] The OpenDSR[370] is an open-source effort that establishes a standard framework for businesses to collaborate on the fair and transparent use of user data while respecting data subject rights relating to personal data requests as outlined in the GDPR and the CCPA. My Data Done Right is a project that assists data subjects in the Netherlands create, send, and track requests to access, delete, update, or relocate their data[371]. No assurance utilising these solutions/techniques would help data subjects better exercise their rights or verify that data controller are compliant because they are not approved by regulating authorities.[372]

3. DATA LOCALISATION

Due to the lack of international consensus on a global regulatory framework for cross-border data flows, many nations are driven to enact restrictive data-flow legislation and policies to overcome digital economy market risks and defend local values and interests. Data localisation regulations are progressively expanding all over the globe while disrupting data flows and, at the same time, reducing commerce, lowering production efficiency, and increasing costs for companies and consumers. Aspirations for data localisation have grown as some policymakers unwittingly embrace it since they do not comprehend how businesses manage data on a global platform while adhering to appropriate regulations. Therefore, as a type of protectionist policy, more policymakers actively advocate localisation and use technical

[368] CPA (2020), "*Implementing Data Portability: Lessons for a Made-In-Canada Approach*", p.22. Available at: https://www.cpacanada.ca/en/public-interest/public-policy-government-relations/policy-advocacy/data-governance/data-portability; [Accessed on 23 January 2022];
[369] Ibid, p.23;
[370] OpenDSR, available at: https://opendsr.org/; [Accessed on 25 January 2022];
[371] My Data Done Right; Available at: https://www.mydatadoneright.eu/about; Accessed [25 January 2022];
[372] Wong J., Henderson T. (2019), *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, (n.350), p.18;

and administrative rules and other restrictions to compel data localisation[373]. By attempting to place data under state control and enable the government to identify and harass individuals, data localisation aids political repression. This compromises privacy, data protection, and freedom of expression.[374] As a result, data flow restrictions may be a vital component of a country's protection of national security e.g. against illegitimate foreign surveillance and a valuable tool for monitoring its citizens' digital activities. This concept highlights PRC's[375] approach to data flow control, extending far beyond technical security issues to concerns about societal stability, technological identity, and political or economic domination. The restricted approach taken by the PRC has gained traction in other countries such as Vietnam[376], Kazakhstan[377], and Indonesia[378]. In these nations, data protection typically refers to data/information security rather than preserving individual' privacy rights.

Several cross-border data transfer restrictions can be regarded through the prism of national security. The fundamental reason for a limited approach is the unique political and societal setting. However, a government may use other bases to justify data restrictions under the national security exemption. In terms of data transfer, three specific reasons are likely to affect the majority of countries, such as:[379]

- *Cyber espionage*: Governments can find it more challenging to monitor interactions deemed of national security significance by restricting data flow crossing the border. Moreover, restrictions on data necessary for national security may raise the cost of cyber espionage activities, particularly in circumstances where corporations are legally required to send over any data through the country to the government. Therefore, the risk of cyber espionage remains prevalent even

[373] Cory N., Dascoli L., (2021) "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" (ITIF, 2021); Available at: https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost**;** [Accessed on 23 January 2022]

[374] Erica Fraser, "Data Localisation and the Balkanisation of the Internet," *SCRIPTed*, 2016, Vol. 13, p. 359, Available at: https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/; [Accessed on 27 January 2022];

[375] Chander, Anupam and Le, Uyen P.*(2014), Breaking the Web: Data Localization vs. the Global Internet*, Emory Law Journal, Forthcoming, UC Davis Legal Studies Research Paper No. 378, p.8. Available at SSRN: https://ssrn.com/abstract=2407858; [Accessed on 27 January 2022];

[376] Ibid,p.23

[377] Ibid,p.25

[378] Mitchell, A. D. and Hepburn, J. (2017), Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer. 19 Yale Journal of Law and Technology 182, Available at SSRN: https://ssrn.com/abstract=2846830; [Accessed on 28 January 2022];

[378] Chander, Anupam and Le, Uyen P.*(2014), Breaking the Web: Data Localization vs. the Global Internet*, (n.375),p.23;

[379] Ferracane, M.F. (2019), "Data flows and national security: a conceptual framework to assess restrictions on data flows under GATS security exception", Digital Policy, Regulation and Governance, Vol. 21 No. 1, pp. 44-70.p.53. Available at:https://doi.org/10.1108/DPRG-09-2018-0052; [Accessed on 26 January 2022];

when data is handled locally, as cyber espionage is typically performed remotely today.[380]

- *Cyberattacks on critical infrastructure*: By limiting data flow, critical infrastructure is stronger and more resistant to cyberattacks. There is no universal definition of critical infrastructure since countries have different priorities when determining what is genuinely critical (e.g. energy, telecommunication, financial services, security services etc.). These sectors will become even more prone to cyber threats as the IoT and 5G technologies progress. One example of legislation applied to critical infrastructure that restricts data transfers on the premise of national security is the Cybersecurity Law in the PRC. On the other hand, implementing solid security standards and encryption techniques is a more practical approach to improving critical infrastructure resilience and ensuring a better response to cyber attacks than data localisation.[381]
- *Terrorist threats*: Storing data locally can increase a government's ability to undertake domestic surveillance to identify potential hazards and prevent terrorist acts. Governments have frequently emphasised the inadequacies of the current process for demanding access to data stored across the border to investigate terrorist threats. A network of MLATs is the existing framework for obtaining evidence and law enforcement objectives overseas, including investigating terrorist acts. The U.S. CLOUD Act was created to make it easier for governmental agencies to access data to avoid terrorist threats.[382]

Even though these stated reasons for introducing data locations are based on national security, data localisation and the ensuing internet fragmentation have national security repercussions, including repressive threats to democracy, limitations on security actors' collaboration and competence, and fears about cybersecurity.

Countries persist in referencing law enforcement and regulatory issues about cross-border access to data as reasonings for data localisation and digital protectionism. Some jurisdictions support data localisation because efficient cross-border law enforcement methods are scarce. If data is stored domestically, government agencies will be unable to stall investigations by trying to prevent providers from meeting government demands. Data collected for law enforcement localisation is frequently the result of legislators' unwillingness

[380] Ibid, p.56;
[381] Ibid, p.57-59;
[382] Ibid, p. 60;

to confront the underlying challenges with current legal techniques to enhance the process of creating cross-border requests for data. Data security is primarily determined by the control mechanisms used to safeguard it, such as encryption technology and security for data centres. The ethnic background of those who own or control servers or where devices are located is not crucial for their protection. Data security is governed by the service provider's technical, physical, and administrative rules, which can be good or bad depending on where the data is stored.[383] The more the Internet is localised, the fewer benefits. There are numerous methods for controlling data flows, some more stringent than others. Some type of agreement where the sensitivity of the data is balanced with its functionality and valuation and regulatory requirements generating accountability for data sources, data transfer, storage, and processing may be helpful on a case-by-case, country-by-country basis. In some cases, localisation is more of a political issue than an economic or social one.[384]

3.1. DIRECT DATA LOCALISATION

All direct data localisation indicators aim to ensure that data is located, stored, processed, and made available within a specific national or regional territory. They typically appear as a component of data protection or information security legislation. For example, the Cybersecurity Law of the PRC is concerned with information security and critical infrastructure.[385] Personal and important data acquired and created by essential information infrastructure operators in the PRC must be stored domestically under this law[386]. In Sweden, financial documents must be physically stored domestically for seven years. In ICT contracts, specific federal U.S. government agencies command the use of a specialised U.S. based cloud service (hereinafter "GovCloud") and define local data storage. The U.S. government agencies use GovCloud for sensitive tasks that must adhere to strict compliance standards, such as the International Traffic in Arms Regulations, the Federal Risk and Management Program, the Department of Defense Security Requirements Guide and Criminal Justice Information Services. The Amazon Web Services (hereinafter "AWS") GovCloud territories are located in

[383]Cory N., Dascoli L.,(2021) "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them", (n 373);
[384] Taylor, R.D. (2020) '"Data localization": The internet in the balance', Telecommunications policy, 44(8), p. 102003. Available at: https://www.sciencedirect.com/science/article/pii/S0308596120300951; [Accessed on 26 February 2022];
[385] Livingston S., 'China set to expand data localisation and security review requirements' (IAPP Privacy Tracker, 25 April 2017) [Accessed on 29 January 2022];
[386] Article 36. of the Cybersecurity Law of the PRC;

the U.S. and are managed physically and functionally by AWS personnel who are only U.S. citizens. They are physically separated from the rest of the Amazon Web Services cloud areas. This requirement for localisation is contractual.[387] According to the Accounting Act in Finland[388], a copy of accounting records must be stored in Finland. The data can be stored in another EU member state if immediate access is guaranteed.[389] The German Telecommunications Act states that telecommunications providers must store data on phone numbers, the time and place of communications (except for emails), and involved IP addresses for four to 10 weeks on servers within Germany.[390]

3.2 INDIRECT LOCALISATION

Localisation can also be indirect. Data localisation, for example, can be an inherent consequence of a certain kind of provision. Legislation may, for instance, demand the installation of additional protection measures, such as a set of contractual conditions, before data is transferred across borders. The data subject's consent for cross-border transfer is the most prevalent condition. This condition, like most others, might be more or less stringent, and its interpretation or execution may differ. In theory, the primary goal of data protection legislation is to protect personal information, which does not always imply data localisation. Data protection rules, on the other hand, frequently negatively impact data flows and might be considered implicit localisation measures. They do not stop international data transfers altogether but make them more complex. In some countries, data protection is viewed as a human rights problem, and it cannot be equated to the economic character of other localisation initiatives. As a result, such measures should be seen as a separate issue stemming from human rights legislation and social compact rather than any techno-nationalist or protectionist tendencies. They should not be addressed through trade regulations. Furthermore, privacy protection differs from direct localisation and obstacles in that the problem would be resolved

[387] Cory N., Dascoli L., "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them", (n 373) ; *see* "What Is AWS GovCloud (US)?" AWS website, https://docs.aws.amazon.com/govcloudus/latest/UserGuide/whatis.html; "AWS GovCloud (US)," Available at: https://aws.amazon.com/govcloud-us/?whats-new-ess.sortby=item.additionalFields.postDateTime&whats-new-ess.sort-order=desc; [Accessed on 26 January 2022];
[388] Section 9 (30.12.2004/1304) of the Accounting Act 1336/1997;
[389] Available at: https://ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy/; [Accessed on 29 January 2022];
[390] Rich C.(2017), "A Look at New Trends in 2017: Privacy Laws in Europe and Eurasia (non-EEA),", Bloomberg Law, Available at: https://media2.mofo.com/documents/170717-privacy-lawseurope-eurasia.pdf; [Accessed on 29 January 2022];

if a foreign country to whom data is transported adopted stricter privacy legislation. Because data localisation can have a detrimental influence on data flows and limit data subjects' ability to choose how their data is processed, it is crucial to ensure that data protection rules aren't being exploited to enforce protectionist policies. Under the GDPR, personal data may be freely transferred between EEA countries and select jurisdictions deemed adequately secure in terms of data protection. The LPDP in Bosnia and Herzegowina states that explicit consent, contractual need, and vital interest are among the grounds for transferring personal data cross-border to a state deemed inadequately safe. Due to the lack of a codified list of countries which Bosnia and Herzegovina considers secure, the individual data controller must make this assessment.[391]

4. DATA – ACCESS CONTROL MECHANISMS

Like personal data, private-sector data often need more stringent access controls than non-personal public-sector data, commonly shared through open data. Access control mediates each request to a system's resources and data and determines whether the appeal should be allowed or refused.[392] A method applying regulations specified by a security policy enforces the access control decision. Different access control rules can be implemented, correlating to diverse criteria for identifying what should and should not be allowed and different views of what security implies.[393] This is referred to as access control. The construction of an access control system necessitates the specification of the rules that will govern access and their implementation as computer-executable functions. It is one of the essential techniques for protecting personal data from unauthorised access, misuse, and other risks.

The performance of a suitable mechanism is compounded by the need to deal with any security flaws caused by the implementation itself and the challenge of translating access control mechanisms to a computer system.[394] The access control mechanism must function as

[391] Article 18 of the LPDP of BiH;
[392] OECD (2019), Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies, (n 6),p.32;
[393] Samarati, P. and de Vimercati, S.C. (2001) 'Access Control: Policies, Models, and Mechanisms', in Foundations of Security Analysis and Design. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 137–196.p.137 ; Available at. https://link.springer.com/chapter/10.1007/3-540-45608-2_3;
[Accessed on 30 January 2022];
[394] Ibid;

a reference validation mechanism[395], i.e. a trustworthy component intercepting all system requests. The access control mechanism must always control all systems and resource accesses and be contained to a specific system section. Moreover, they need to be impenetrable to tampering because tampering with the reference validation method destroys its validity, as does any prospect of gaining security.[396] Access control mechanisms can be classified into three types:[397]

- *Discretionary Access Control (DAC)*: represents a mechanism of control access depending on the identification of the persons attempting to process or access data;
- *Role-Based Access Control (RBAC):* the assignment of roles and the rules that govern what access is provided to individuals in particular positions. Frequently utilised in large-scale businesses where several work groups or departments with separate functions are interconnected.
- *Mandatory Access Control (MAC)*: This access mechanism supplements the preceding ones by adding an added level of security for access control. MAC works by marking every element in the system, which will subsequently be subject to the access control policies that have been established.

According to the OECD[398], *(ad hoc) downloads* are one of the most common mechanisms to access data, which increases digital security and privacy problems since data, once downloaded, is no longer under the control of the data owners. Data is downloaded and preserved, preferably in a commonly used format, before being made accessible online. The following mechanism to control data access is *Application programming interfaces(API)*. APIs enable service providers to make their digital resources accessible to the general public via the Internet. APIs allow the seamless interconnection of several actors, platforms, and services, mainly through cloud computing. Data owners can also use APIs to limit how their data is used, including procedures for data portability. They also have control over the API user's identity, the amount and scope of data used, and even the extent to which the information generated from the data may disclose sensitive/personal information.[399] Finally*, data sandboxes* are

[395] Anderson P.(1972), Computer security technology planning study. Technical Report ESD-TR-73-51, Volume 1, p.9. Available at: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande72a.pdf; [Accessed on 06 January 2022];
[396] Ibid;
[397] Samarati, P. and de Vimercati, S.C. (2001) '*Access Control: Policies, Models, and Mechanisms*', in *Foundations of Security Analysis and Design,* (n 393), p.138;
[398] OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, (n 6),p.32;
[399] Ibid;

regarded as a way of gaining access to sensitive and propriety data while preserving rights holders' privacy and intellectual property rights. They describe any scalable and developmental platform in which data may be read and processed, and analytic outputs are exported only when they are non-sensitive. As a result, data sandboxes have the potential to facilitate access to sensitive/personal and proprietary data.[400]

Therefore, data access control mechanisms are technological and organisational procedures that enable authorised users to access data safely and securely inside and beyond organisational boundaries while safeguarding actors' rights and interests and adhering to relevant regulatory frameworks. It is one of the essential techniques for protecting personal data from unauthorised access, misuse, and other risks.[401]

5. BENEFITS OF DATA SHARING

The Covid-19 pandemic highlighted the significance of data usage and data flows. As countries implement different measures, access to digital solutions and services, which rely on national and international data flow, becomes crucial. However, data on its own has no value and is only valuable if the parties can use it to highlight their position in services based on market data. Not all data is the same, and different forms of data may necessitate different approaches. Data is a form of assets that can never be depleted and can be reused for an indefinite variety of purposes by different parties, including those that could not have been projected when the data was created without reducing its value.[402] To achieve the social and economic value of data, it is essential to convert it into information and then knowledge through analysis so that it can be used in decision-making by businesses and society. Businesses depend on cross-border data flows to innovate, increase production, and globalise business activities. Data regarding transactions and consumer preferences in different locations is essential for distributing digital and commercial services. Additionally, data flows can encourage government cooperation to improve international policies.[403] Since data is an

[400] Ibid,p.33;
[401] OECD (2021), Recommendation of the Council on Enhancing Access to and Sharing of Data, Available at: https://legalinstruments.oecd.org/Insnments/instruments/OECD-LEGAL-0463; [Accessed on 06 January 2022] ;
[402] Martens, de Streel, A., Graef, I., Tombal, T., & Duch-Brown, N. (2020). Business-to-business data sharing: An economic and legal analysis. European Commission. p. 12. Available at: https://joint-research-centre.ec.europa.eu/document/download/c48fbb97-7e53-4082-a5a1-9a4ad1b6577c_en?filename=jrc121336.pdf; [Accessed on 11 January 2022];
[403]OECD (2020), OECD Digital Economy Outlook 2020, (n 146);

important factor of the digital economy and can provide considerable development gains to a variety of businesses and society, data sharing is beneficial to increase positive impacts while minimising potential risks.[404]

Unfortunately, because of considerable imbalances in market power, most of the benefits of data sharing and cross-border data flow have developed countries, while developing countries, except the PRC, are only mere providers of raw data for global digital platforms. [405]

The continuous movement of data across international borders underpins global economic activity and is vital to advancing technologies like AI and the IoT. These technologies support productivity and competitiveness and address many societal challenges, which implies potential benefits for both the public and private sectors. Data is also essential for knowledge-based economies, and access to them is the main factor for social and economic policies.[406] Access to data and scientific collaboration is necessary for researchers to provide solutions to current and emerging social, environmental, and economic challenges. Moreover, access to and exchange of health data is needed to discover and improve new treatments and raise healthcare standards.

For future development and well-being, it is necessary to optimise access and data sharing, establish privacy regulations to enable cross-border data flows, and open up government data to encourage digital innovation.

IV. BARRIERS TO DATA SHARING AND RE-USE

Cross-border data flows pose many risks to individuals and businesses, including violating privacy and other legitimate private interests.[407] A considerable share of the world's data and processing will be transferred internationally to reflect the worldwide allocation of economic and social online activities.

Data flow have an international dimension, enabling trade between countries and global competition among data market actors and contributing to more significant mutual commitment and cross-border efforts to promote greater public transparency and contribute

[404] UNCTAD (2021), *Digital Economy Report - Cross-border data flows and development: For whom the data flow*, (n 2), p.65;
[405] Ibid, p. 84;
[406] OCDE. (2020). *Mapping approaches to data and data flows*. Organisation for Economic Cooperation & Development, p.10; Available at:https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf.; [Accessed on 10 January 2022] ;
[407] OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, (n 6);

significantly to economic expansion. Therefore, transborder data flows are required to transfer data and knowledge and move globally dispersed data markets and societies. . Furthermore, cross-border data flows can enhance government cooperation to improve international policymaking and identify global impediments.

Restrictions on cross-border data flow may limit market functioning and societal prosperity by limiting the benefits of cross-country sharing and re-using data, information, and knowledge.[408] The political, organisational, legal, technical, and economic barriers[409] are frequently related and dependent on one another. The lack of cross-border data sharing standards, access control mechanisms, protection of intellectual property rights and data ownership complicate cross-border data sharing. Compliance with various national legislations is complicated.[410] Cross-border data restrictions can be based on various legal grounds, including data security, data sovereignty, and law enforcement.

Even though data sharing is beneficial, it raises substantial concerns. Finding the right compromise between making data accessible and protecting privacy, ensuring access, determining ownership of the data, and protecting IPR with all potential risks is necessary. Restrictions must be proportionate to all possible risks to achieve the best results.[411] The proportionality assessment should be made on a case-by-case basis with respect to human rights and the rule of law.[412]

---

[408] Ibid;

[409] Political barriers stress the importance of political differences between countries. Restrictive data access control policies, administrative obstacles, a lack of political will, a lack of awareness among governments or public administrations, and a country's political structure are examples of political barriers to data sharing. Such barriers obstruct successful sharing on a global platform.
Organisational barriers include internal and external factors and the skills required to work with data to fulfil its potential.
Technical barriers, such as a lack of standardisation and common access protocols, varying data quality, database incompatibility, and language barriers, significantly impact data sharing and re-use.
Economic barriers to data sharing occur when a country or institution lacks financial resources and skilled personnel due to limited training and challenges in retaining employees. Data sharing may also have a negative economic impact by reducing trade and travel.
See Berends J., Fechner T., Carrara W.(2020), *Analytical Report 5: Barriers in working with Open Data,* Luxembourg: Publications Office of the European Union, p.17-22, Available at: https://data.europa.eu/sites/default/files/edp_analytical_report_n5_-_barriers_in_open_data.pdf; [Accessed on 30 January 2021];

[410] Edelstein, Michael & Sane, Jussi. (2015). *Overcoming Barriers to Data Sharing in Public Health: A Global Perspective*. p.8, Available at: https://www.chathamhouse.org/sites/default/files/field/field_document/20150417OvercomingBarriersDataSharingPublicHealthSaneEdelstein.pdf

[411] OECD (2020), Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, amended on 11 July 2013, OECD, Paris, Available at: https://legalinstruments.oecd.org/public/doc/114/114.en.pdf; [Accessed on 28 January 2021];

[412] OECD (2011), Recommendation of the Council on Principles for Internet Policy Making, OECD, Paris, Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0387; [Accessed on 27 February 2022];

1. DATA SECURITY AND LACK OF COMMON STANDARDS

As more countries implement data protection legislation, some authorities support data localisation because they believe storing data within national borders is the best way to secure it. Keeping data domestically does not always minimise exposure to intrusions. Data security results from the technologies and standards employed in data-driven industries. Moreover, mandating data localisation in nations with insufficient digital infrastructure may jeopardise data security. Strong privacy and cybersecurity standards, on the other hand, can assist in securing data from all kinds of risks regardless of where it is stored. [413] The nationality of those who own or operate servers, or the country where these machines are situated, has nothing to do with their security. For example, the DSL of the PRC imposes additional obligations on businesses that engage in actions that may endanger national security, public interest, or legitimate interests of persons or businesses. In this case, according to DSL, data processors must get licenses and collaborate with national security authorities during the data review procedures[414].

Domestic data sets make it more difficult for businesses to detect patterns in illegal conduct. Numerous cross-border data flow regulations are set to ensure that all data transferring across borders obtains the same level of data protection, security, and privacy as data flowing within the jurisdiction (e.g. GDPR). This is extremely difficult to execute in LDCs and other developing countries due to a lack of implementation capacity.

The lack of common standards is one of the most commonly stated impediments to data transfer and re-use. Inconsistent data standards, for example, impede the production of continuous data sets because modifications in assessment and collecting techniques make it difficult to evaluate and aggregate data. Standards are essential for interoperability, which is not always guaranteed even when commonly used machine-readable formats are employed for availability.[415] Furthermore, data-sharing initiatives (e.g. the CORBEL Initiative[416]) have ignored current data standards and implementation techniques, increasing the problem of compatible standards and a lack of harmonisation that may jeopardise the adoption of common

[413] Cory, N. (2017). *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*.ITIF, P.4. Available at: https://www.researchgate.net/publication/333292633_Cross-Border_Data_Flows_Where_Are_the_Barriers_and_What_Do_They_Cost [accessed 03 March 2022];
[414] Ibid, p.17;
[415] OECD (2019), *Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*, (n 6);
[416] CORBEL - Coordinated Research Infrastructures Building Enduring Life-science Services. Available at: https://www.elixir-europe.org/about/eu-projects/corbel. [Accessed on 26 January 2022];

global standards.[417] The International Organisation for Standardization (hereinafter "ISO") has created a privacy protection ISO (ISO/IEC 27701:2019) that defines standards and provides guidance for developing, executing, maintaining, and continuously improving a PIMS. It is essential to use and embrace comprehensive data standards to overcome interoperability and data sharing challenges that increase expenses and impede accessibility[418]. Common data standards, committed to adequately regulated terminology and familiar concepts and harmoniously integrated into a global network, can play an essential part in addressing the general problem of data sharing. Nevertheless, political obstacles must also be removed, and broad collaboration across all organisations must be established.[419]

2. DATA SOVEREIGNTY

Regarding data and its cross-border flow, the traditional concept of sovereignty, linked to the national territory and physical borders, is inappropriate. In particular, the Internet is designed as decentralised and borderless and has a crucial role in collecting, processing, and sharing data. Furthermore, as data become a vital part of economic growth and countries face a loss of control over them in cross-border transmission, concerns about data sovereignty are increasing.[420] Despite the benefits of the Internet and cross-border data flow, many countries are introducing limitations measures that produce extraterritorial or only national effects, depending on the norm-setting power and intent of the initiator.

Data sovereignty is a strategy for resuming state authority and self-determination[421] in the digital ecosystem. It has been used to safeguard different processes designed to increase data ownership and autonomy.[422] The primary goal of data sovereignty measures is to ensure the applicability and robust enforcement mechanisms of national laws by establishing some correlation with the territory. Different approaches to data sovereignty depend on national

[417] R.D. Kush, D. Warzel, M.A. Kush, A. Sherman, E.A. Navarro, R. Fitzmartin, F. Pétavy, J. Galvez, L.B. Becnel, F.L. Zhou, N. Harmon, B. Jauregui, T. Jackson, L. Hudson (2020*), FAIR data sharing: The roles of common data elements and harmonization*, Journal of Biomedical Informatics, Volume 107, ISSN 1532-0464, p.2; Available at: https://doi.org/10.1016/j.jbi.2020.103421; [Accessed on 30 January 2021];
[418] Ibid, p.8;
[419] Ibid;
[420] UNCTAD (2021), *Digital Economy Report - Cross-border data flows and development: For whom the data flow*, (n 2), p.86;
[421] Switzerland is the first country to adopt the concept of digital self-determination. The concept of digital self-determination promotes the creation of secure data environments based on democratic principles.
[422] De La Chapelle B. and Porciuncula L (2021). *We Need to Talk About Data: Framing the Debate Around the Free Flow of Data and Data Sovereignty*. Internet & Jurisdiction Policy Network (I&JPN), Paris. p.36 Available at: https://www.internetjurisdiction.net/news/aboutdata-report; [Accessed on 23 January 2022];

priorities, ranging from protecting human and economic rights to advancing societal objectives. Even though state policies to obtain data sovereignty can have a positive outcome, they can have a detrimental effect involving excessive constraints, which can take the form of data localisation. The impact of data localisation provisions largely depends on whether they apply to all data or only special categories or whether they build a complete prohibition on cross-border transfer.

Requests for data sovereignty and strict data localisation requirements are increasingly shaping European viewpoints on "*digital sovereignty*".[423] The EU has navigated its digital sovereignty toward „strategic autonomy", which indicates that the state is not constrained to an unfavourable extent by digitalisation dependencies when integrating its own political, social, and economic priorities.[424] The European Union does not formally support data localisation in its regulations. Although the GDPR stresses the significance of cross-border flows of personal data, the GDPR's strict requirements prevent an easy path for cross-border data flows. Furthermore, the Data Management Act, the CJEU decision in the *Schrems II case*, and the GAIA-X initiative[425] point to a shift in attitude toward the localisation of EU data.[426] In the United States, data sovereignty is primarily the result of private-sector business decisions.[427] The PRC's digital/data sovereignty approach is centred on global technological leadership and data protection, i.e. positioning digital technology as a geopolitical advantage.[428]

Hence, data sovereignty measures must obtain a balance of competing interests through the extensive network of interconnected regulations. Each of these provisions can have significant ramifications when implemented. Finally, various data sovereignty measures are constantly changing and subject to complex rules, implying more conflicts of laws and making integration and cooperation even more difficult.[429]

---

[423] Christakis T., *"'European Digital Sovereignty': Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy'*, Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute, e-book, December 2020, p. 65; Available at https://ssrn.com/abstract=3748098 & https://airegulation.com; [Accessed on 23 January 2022];

[424] Ibid;

[425] More information is available at: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html: [Accessed on 30 January 2022];

[426] UNCTAD (2021), *Digital Economy Report - Cross-border data flows and development: For whom the data flow*, (n 2), p.107;

[427] Daskal, J. (n.d.). The Opening Salvo: The CLOUD Act, e-Evidence Proposals, and EU–US Discussions Regarding Law Enforcement Access to Data across Borders. In (pp. 319-341). p.325 Available at: https://doi:10.1017/9781108755641.012; [Accessed on 17 January 2022];

[428] UNCTAD (2021), *Digital Economy Report - Cross-border data flows and development: For whom the data flow*, (n 2), p.86;

[429] De La Chapelle B and Porciuncula L (2021). *We Need to Talk About Data: Framing the Debate Around the*

3. LAW ENFORCEMENT

Countries have implemented a variety of regulatory measures in response to the expanding volume of cross-border data. However, several issues have emerged from the latest cross-border data expansion for the national authorities. One of them is guaranteeing law enforcement access to data, which has contributed to enforcing data localisation requirements. Current regulatory solutions are inadequate for dealing with information-related issues. Data governance standards and their relationship with law enforcement provide regulatory tools for authorities to handle their law enforcement commitments while ensuring that internet providers are not punished unjustly. Legislators' failure to address fundamental problems in present legal mechanisms to improve the process of making cross-border data requests commonly leads to law enforcement-motivated data localisation.

Because crime and digital services have an international nature, governments will eventually seek help from other nations, even if localisation restrictions exist.[430] According to an assessment in the EU, electronic evidence is significant in around 85 % of overall criminal investigations, and 55% of investigations involve cross-border access to electronic evidence.[431] Authorities in the PRC, Turkey, and other countries use this justification for data localisation without proving its advantages. When law enforcement authorities need to access data held in a foreign country but lack the powers to compel the internet provider to deliver the data, tensions develop. In that event, courts may fail to get essential information, perhaps leaving a case unresolved or resorting to harsh measures that excessively burden service providers and negatively affect consumers, hampering the global digital economy.

Mutual Legal Assistance Treaties (hereinafter "MLATs") are the primary foundation for international law enforcement cooperation. Generally, MLATs have concentrated on criminal and public investigative processes such as collecting testimony from witnesses based overseas, executing search warrants in other jurisdictions, and obtaining records from foreign financial institutions. Recent cases demonstrate the issues that global data flows can pose for law enforcement, such as the *Microsoft Ireland Case*[432]*,* which emphasises the fundamental jurisdictional problems presented by law enforcement's interest in data situated across borders. In this case, the U.S. government wanted information kept by Microsoft in Dublin,

Free Flow of Data and Data Sovereignty, (n 422);
[430] Cory, N. & Dascoli, L. (2021). How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them, (n 373);
[431] Ibid;
[432] United States v. Microsoft Corp. (Microsoft Ireland), No. 17-2, slip op. at 3 (Apr. 17, 2018);

Ireland. Several district judges held that, despite being located outside the United States, the data was in the possession and control of a U.S.based provider and thus subject to the warrant authority issued under the Stored Communications Act (hereinafter "SCA")[433]. The Second Circuit overturned the decision and held that the location of the data, rather than the location of the provider accessing the data, was the fundamental indicator of territoriality and jurisdiction. According to this judgement, the U.S. government has jurisdiction over data stored inside U.S. territorial jurisdiction, but the Irish government has authority over data maintained within Irish territorial jurisdiction. If the U.S. wants data from Dublin, it must submit a diplomatic request, just as the U.S. would if Irish law enforcement wanted data in the United States. The case was brought to the United States Supreme Court but concluded without a verdict on March 23, 2018, due to the enactment of the new CLOUD Act. The CLOUD Act permits federal law enforcement to compel U.S.-based technology businesses to produce requested data kept on servers by warrant or subpoena, regardless of whether the data is hosted in the United States or on foreign ground.[434] Moreover, under the Electronic Communications Privacy Act (hereinafter " ECPA")[435], U.S. law enforcement has access to both domestic and overseas user data, including communications content. Title II of the ECPA, the SCA, governs law enforcement access to user data, content information (e.g. e-mail), and non-content information (e.g. transactional or subscriber information) and defines the requirements for releasing user information using search warrants, subpoenas[436] or court orders[437]. While the SCA initially allowed law enforcement to access user material by a subpoena if the data had been kept for more than 180 days, it is now widely acknowledged that law enforcement must obtain user content with a warrant.

The combination of cross-border data flows and law enforcement illustrates the difficulties that new technology might provide for authorities. New modes of information exchange and their vast amount, unfathomable only a decade ago, offer tremendous industry prospects. Therefore, new legal procedures are required to increase the efficiency of data

[433] Stored Communications Act, Pub. L. 99-508, tit. II, 100 Stat. 1848, 1860-68 (1986) (codified as amended at 18 U.S.C. §§ 2701-12);
[434] Molinuevo, M. And Gaillard, S. J. H.(2018), *Trade, Cross-Border Data, and the Next Regulatory Frontier : Law Enforcement and Data Localization Requirements* (English). MTI Practice Note,no. 3 Washington, D.C. : World Bank Group. P.5. Available at: http://documents.worldbank.org/curated/en/903261543589829872/Trade-Cross-Border-Data-and-the-Next-Regulatory-Frontier-Law-Enforcement-and-Data-Localization-Requirements; [Accessed on 01 February 2022];
[435] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–2522 (2012);
[436] 18 U.S.C. § 2703 (2012);
[437] 18 U.S.C. § 2703(d);

exchange for law enforcement aims, while protecting privacy. Examples include the EU-U.S. Umbrella Agreement, the EU-U.S. Terrorist Finance Tracking Program Agreement, and the UK-U.S. CLOUD Act agreement[438]. They generally acknowledged global privacy principles while considering local interpretation and regulatory regimes. In general, they work without interfering with data flows.[439]

4. THE IMPLICATION OF BARRIERS TO DATA SHARING

To construct digital border controls, existing data localisation measures employ a combination of cross-border data flow restrictions and local storage requirements. Because there is a lack of understanding about how businesses use data, how data travels across borders, and how data regulation may influence businesses, assessing the impact of various data localisation measures can be challenging. Nevertheless, it is noticeable that restricting data flows has significant implications on a country's economy, considerably reducing overall trade volume, decreasing productivity, and increasing prices for industries that rely on data while imposing regulatory burden or favouring domestic over international businesses. The COVID-19 pandemic emphasised the significance of data flows in the global economy, enabling economic (e.g., the use of digital services for businesses), health (e.g., data sharing for medical research), and societal responses (e.g., video calls, online shopping). Barriers to data flow focus on a rising number of specific data types and broad categories of data considered sensitive or relevant to data protection or national security. Additional safeguards, such as standard contractual clauses or consent, are necessary for each personal data transfer, imposing substantial administrative costs and delays. Some countries explicitly advocate for data localisation as part of digital protectionism, while others hide localisation and protectionism behind technical rules.[440] Data localisation compromises user privacy by giving foreign governments more access to personal information, reducing corporations' capacity to defend fundamental rights overseas, and monopolising the market for privacy measures. Data is

[438] Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, USA No. 6 (2019); Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf; [Accessed on 04 February 2022]

[439] Cory N. And Dascoli L.(2021), *How Barriers To Cross-Border Data Flows Are Spreading Globally, How Much They Cost, And How To Address Them*, (n 373);

[440] Ibid;

directly under the authority of a government when it is contained inside a geographical jurisdiction, allowing the government to modify access restrictions at will.[441]

On the other hand, through increased confidence in digital products, data-related restrictions can have a positive impact. Companies and consumers may be more eager to employ Internet solutions if they are required to store data locally. However, data flows will increase as more governments and organisations embrace digital transformation. Restricting data flow has little impact on social or economic benefits and may contribute to the perception of data protection as primarily administrative, with little real help to data subjects. This can result from a reduction in informational asymmetries between consumers and businesses and a decrease in adverse selection. As discussed in the following sections, finance and commerce, health care, and ICT are the primary industries where data flow restrictions are most noticeable.

4.1. FINANCIAL SERVICE AND (E-)COMMERCE SECTOR

The financial services business is primarily data-driven. This is mainly because data quickly becomes a necessary component and foundation for many economic goods and services. It is often considered a crucial *asset* for increasing competitiveness and industry growth. In consumer and business banking, transactions, trading, wealth management, investment banking, and insurance, data is used to evaluate risk, manage finances, forecast market movements, improve investments, maintain financial books and records, and conduct effective communication of trade and payment instructions. As a result, data access and sharing may deliver significant benefits to industry participants while redefining the competitive situation.[442]

Three types of data sharing can assist financial institutions:[443]

- *Inbound data sharing*: entails collecting data from third parties. This data exchange enables institutions to contribute more information to their decision-making processes, resulting in higher-quality outputs and more accurate operations.

[441] Brehmer, H Jacqueline (2018), *"Data Localization The Unintended Consequences Of Privacy Litigation*," American University Law Review: Vol. 67 : Iss. 3 , Article 6.,p.960. Available at: http://digitalcommons.wcl.american.edu/aulr/vol67/iss3/6; [Accessed on 02 February 2022];

[442] Zachariadis M.(2020), "Data-sharing frameworks in financial services: Discussing open banking regulation for Canada" p.2. Available at: SSRN: https://ssrn.com/abstract=2983066 ; [Accessed on 21 January 2022];

[443] World Economic Forum, *The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value (White Paper)*, p. 3. Available at: https://www3.weforum.org/docs/WEF_Next_Gen_Data_Sharing_Financial_Services.pdf; [Accessed on 21 January 2022];

- *Outbound data sharing*: entails exchanging owned data with third parties, i.e. allows institutions to exploit that they would not have in-house. However, sharing data with third parties increases the risk of releasing competitive material that might be used against them.; and.
- *Collaborative data sharing*: entails both inbound and outbound sharing of related data types. Collaborative data sharing allows institutions to collect data on a level they could not otherwise attain, resulting in a volume and quality of findings that would not otherwise be accessible.

Allowing data sharing across borders can bring more national businesses and consumers online, increasing the use of data-driven business strategies and supporting the national economy.

Through data sharing, consumers may reclaim control and ownership of their financial data, resulting in higher-quality goods or more efficient services. This is acknowledged in the UK's Open Banking Standard[444], the EU's Payment Service Directive 2[445] in general, Australia's Consumer Data Right[446], and various Open API laws in Singapore, Hong Kong, and Japan. These standards compel institutions to set up client data for authorised third parties when the consumer demands it, enabling more competition and innovation.[447] Restricting data sharing has been the main instrument to protect consumers' financial and nonfinancial secrecy. The GDPR compels institutions to provide easier access to personal data to consumers kept by institutions regarding financial information. At the same time, the GLBA requires that financial institutions in the U.S. specify how sensitive consumer data is transferred and adopt appropriate safeguards for what is transmitted. Other countries restrict companies from sharing personal information across borders to safeguard national consumer privacy.[448]

Regarding (e)commerce, more severe data restrictions unnecessarily raise and reduce the supply of data-driven products and services such as data analytics, targeted advertising, and technology used to manage global workforces, product networks, and supply chains. Countries that limit data transfers, according to the model, have a reduction in trade volumes, resulting in higher commodity prices due to a shortage of supply. For example, various drafts of India's

[444] Available at: https://standards.openbanking.org.uk/; [Accessed on 01 February 2022];
[445] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC;
[446] Available at: https://www.accc.gov.au/focus-areas/consumer-data-right-cdr-0; [Accessed on 01 February 2022];
[447] Ibid;
[448] Ibid;

National E-commerce Policy expressly call for compelled data localisation as privacy, cybersecurity, and regulatory measure. Data localisation can push away a more innovative and price-competitive service provider, allowing a less expensive or inferior product to gain market share[449]. The PRC and the Republic of South Africa are examples of nations where rising data restrictions are causing higher pricing, decreased commerce, and lower production. However, the global digital economy urgently requires new laws to secure digital trade and data flows. Traditional trade agreements and domestic data, and digital commerce rules are being surpassed by technology and accompanying business practices. Digital trade agreements are an advanced and accessible method of creating collaboration among digital economies at different stages of development (e.g.DEPA). Businesses benefit from the knowledge they gain to share data as part of cross-border e-commerce and innovation. Early regulatory interoperability helps firms in the long term by removing barriers to e-commerce generated by new legislation. The involvement of supervisory authority also builds trust and confidence among governments and consumers that data trade duties do not overlap with regulatory requirements. It can increase monitoring by allowing for data transfer and collaborative investigations.

4.2. HEALTHCARE SECTOR

Technological advancements have enabled people to collect, analyse, and share personal health data to manage and positively impact the health sector. Individuals, public and private health institutions, and researchers generate health-related data. This data is becoming more digitised and relevant for developing novel health therapies, particularly those that use artificial intelligence and machine learning to improve health outcomes.[450] Academics and international authorities have recommended data sharing concerning the ongoing COVID-19 pandemic, and platforms have been established to facilitate the transfer of patient-level data for patients infected with SARS-CoV-2.[451] In all data categories, the potential of sharing data raises worries about vulnerabilities to the privacy of personal information that may identify or be linked to a person.

---

[449] Cory N. And Dascoli L.(2021), *How Barriers To Cross-Border Data Flows Are Spreading Globally, How Much They Cost, And How To Address Them*, (n 373);
[450] Schwalbe N., Wahl B., Song J., Lehtimaki S.(2020), *Data Sharing and Global Public Health: Defining What We Mean by Data,* Frontiers in Digital Health, VOLUME 2, p.1 Available at: https://www.frontiersin.org/article/10.3389/fdgth.2020.612339; [Accessed on 01 February 2022];
[451] Ibid;

Privacy concerns are especially severe concerning patient data, particularly in resource-constrained situations where data systems are fast changing. Because data protection law varies by jurisdiction, ownership, control, and usage concepts must be compatible with respective jurisdictions' regulatory requirements. Moreover, in some cases, regulations may be absent or not enforced. The use and sharing of personal data to respond to global health crises (e.g. COVID-19) without the data subject's consent are also permissible under the GDPR. The GDPR provides for exceptions to the restriction on the processing of special categories of personal data, such as health data when it is necessary for reasons of public interest in the area of public health[452] based on Union or national law or where there is a need to protect the data subject's vital interests[453] as Recital 46 expressly refers to the control of an epidemic[454]. According to the EDPB, Articles 6. and 9. of the GDPR can be used as a legal basis for processing health-related personal data in the public interest[455]. Although accessing and sharing data is in the public interest, it is necessary to do so in a manner that respects and preserves individual fundamental rights, particularly the right to privacy and data protection. The use of mobile monitoring applications to aid with contact tracing in the COVID-19 pandemic has exposed several of these vulnerabilities, with many incidents of data being compromised. Therefore, despite a rising worldwide commitment to the use and sharing of public health data, this may not be easy in practice. Concerns about protecting individual privacy and the capacity to offer safe storage of personal data and information are referred to as privacy and security issues[456]. Health data need to be fully anonymised to overcome these obstacles. Additionally, several fundamental rights can be restricted due to health emergencies, including the freedom of assembly, movement, and right to privacy. These restrictions have been justified because they are required to eliminate COVID-19. In other words, constraints on individual rights are in the public interest.[457]

---

[452] Article 9.2.(i) of the GDPR;
[453] Article 9.2.(c) of the GDPR;
[454] EDPB (2020), Statement on the processing of personal data in the context of the COVID-19 outbreak,p.2. Available at: https://edpb.europa.eu/sites/default/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf, [Accessed on 15 February 2022];
[455] Ibid;
[456] Simpson E., Brown R., Sillence E., Coventry L., Lloyd K., Gibbs J., Tariq Sh.a, Durrant A.(2021), Understanding the Barriers and Facilitators to Sharing Patient-Generated Health Data Using Digital Technology for People Living With Long-Term Health Conditions: A Narrative Review , Frontiers in Public Health, Volume 9, p. 9, Available at: URL=https://www.frontiersin.org/article/10.3389/fpubh.2021.641424; [Accessed on 22 February 2022];
[457] Staunton, C.(2021): Data Sharing and the Public Interest in a Digital Pandemic*, p.2. Available at: VerfBlog, https://verfassungsblog.de/data-sharing-and-the-public-interest-in-a-digital-pandemic/, p.2. Available at: https://verfassungsblog.de/data-sharing-and-the-public-interest-in-a-digital-pandemic/; [Accessed on 30 March 2022];

The societal and economic advantages of data-driven health care and research are substantial. The benefits of data sharing have been generally acknowledged as accessibility and collaboration, consistency of research, cost-efficiency and avoiding repetitions, speeding of research and development, and saving lives through much more integrated and coordinated public health initiatives[458]. Sharing timely data is essential for health research and citizens and patients, from uncovering complicated processes to comprehending and avoiding illnesses to comparing drivers of disease outcomes across communities and improving health care. At the same time, the protection of personal health data, as foreseen by the GDPR, is essential to fulfilling the fundamental right to data protection entrenched in the CFR and creating confidence among people and patients.

4.3. INFORMATION AND COMMUNICATION TECHNOLOGIES (ICTs) SECTOR

In the realm of digital technology, many forms of data are necessary for innovation and process improvement. ICT technologies (such as AI and the Internet of Things) are essential for digitising products and services and digital market empowerment (e.g. FinTech) while acting as a foundation for linking and opening the Internet, allowing for the free flow of data.[459] Digital technologies and data significantly impact international trade by lowering trade costs, simplifying global value chain coordination, disseminating knowledge and inventions across boundaries, and connecting more businesses and consumers internationally[460]. Additionally, data is required to improve competitiveness due to the data ecosystem that defines data value, although personal and sensitive data pose unique barriers to the data flow.

On the one hand, recent advancements in AI, data, and robotics technology and applications have fundamentally questioned ethical norms, human rights, and safety. On the other hand AI, data, and robotics, present great opportunities for increasing productivity, addressing societal and environmental concerns and improving everyone's quality of life.

Therefore, ICT advancement relies on a legal framework of permission-based on law, partially driven by policy, and a slew of industry-driven certification processes and

[458] Simpson E., Brown R., Sillence E., Coventry L., Lloyd K., Gibbs J., Tariq Sh.a, Durrant A.(2021), *Understanding the Barriers and Facilitators to Sharing Patient-Generated Health Data Using Digital Technology for People Living With Long-Term Health Conditions: A Narrative Review* ,(n 456);
[459] OECD (2020), *OECD Digital Economy Outlook 2020*, OECD (n 146);
[460] Ibid, p.27;

standards.[461] Privacy by design may even improve data subjects' confidence, and privacy must be observed from the start of the design process. Data is undeniably a driving force behind ICT advancements. Still, data governance is required for long-term success in managing data access, sovereignty, and privacy.[462] Accessing and reusing raw data created by government agencies is critical for deploying digital innovation and better governance. Frameworks for data governance must be developed to remove barriers to data sharing for digital technologies, allowing all stakeholders to preserve digital sovereignty over their data assets.[463] For example, the new Open Data Directive intends to lower obstacles to the market entrance, improve data availability, and expand business prospects.[464] Data sharing must be done legally while preserving economic interests by resolving technological and legal concerns around data governance and trust-enhancing data-sharing protocols.[465]

[461] Curry, Zillner, S., Metzger, A., Pazzaglia, J.-C., & Robles, A. G. (2021). *The Elements of Big Data Value: Foundations of the Research and Innovation Ecosystem*. (n 265);
[462] Advances in technology can increase the potential for unreasonable intrusion into privacy. See Case of Patel vs Facebook Inc.No 18-15982,2019 WL 3727424, 9th Cir.Aug.8,2019;
[463] Ibid,p.390-394;
[464] OECD (2020), *OECD Digital Economy Outlook 2020*,(n 146) ,p.43;
[465] Ibid;

CONCLUSION

Undisputedly, data and data sharing are essential development engines. The advancement of data processing technology, which allows massive volumes of data to be transferred across national borders, necessitates the development of uniform regulations to protect personal data. Depending on a country's political, economic, social, technological, and cultural values and ideological foundations, the objectives for managing data protection may differ. Furthermore, considering LDCs and other developing countries lack implementation expertise, applying a uniform approach on a global scale is very challenging. Additionally, many governments have implemented data localisation due to the absence of uniform data protection legislation because they believe it to be the only effective method for protecting their citizens' privacy. However, restrictions on data sharing compromise social, economic, and civil rights by limiting consumers' and businesses' capacity to profit from the data and global markets and allowing governments more control over local data. This restriction also endangers important new developments in information technology (e.g. cloud computing, IoT). Although many governments have placed restrictions on data sharing, the significance of data has been recognised, and it is being made available through various binding and non-binding cooperation channels. In order to achieve optimal outcomes, restrictions on cross-border data flow must be proportionate to all potential risks, taking into account the processing's context, purpose, and sensitivity. Regardless of the challenges of foreseeing the effects of data usage, re-use, and transfer or detecting when the activity may have negative consequences, different groups of actors must make efforts to prevent this. The case law also demonstrates that individuals have the right and responsibility to mandate that their data be kept private and protected when transferred across borders. No data localisation or restriction of sharing data across borders will be necessary if the requisite administrative, physical, and technological protections are in place. Transparent rules, standards, and improving the interoperability of privacy frameworks would significantly increase data sharing proficiency and ensure that technological advancements benefit society. Territoriality should not be the only way to get a password and log in to the data centre that conceals numerous benefits for individuals, businesses, and countries. Security concerns need to be handled using a risk-based rather than a location-based strategy. Achieving a balance between data sharing and data protection is essential.

BIBLIOGRAPHY

EU Legislation and proposals

Council of Europe. (1981), Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (ETS 108);

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC;

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*, OJ L 194, 19.7.2016, p. 1–30.*

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*, OJ L 194, 19.7.2016, p. 1–30.*

Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016, L 119, p. 89).

Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information, PE/28/2019/REV/1, *OJ L 172, 26.6.2019, p. 56–83;*

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p.37;

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information, *OJ L 345, 31.12.2003, p. 90–96;*

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the European Union L 105, 13.4.2006., pp. 54-63;

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, OJ 1995 L 281/31;

European Commission, "Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act*)",* COM(2022) 68 final 2022/0047 (COD);

European Commission, "Proposal for a Regulation of the European Parliament and of the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act)", *COM(2022*) 46 final 2022/0032 (COD).

European Commission, "Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts", COM/2021/206 final,

European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM/2020/825 final;

European Commission, "Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)", COM/2020/842 final;

European Union (2012), *Consolidated Version of the Treaty on the Functioning of the European Union*, , 2012/C 326/01;

European Union (2016), Charter of Fundamental Rights of the European Union, 2016/C 202/02;

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of

personal data by the Community institutions and bodies and on the free movement of such data (OJ 2001, L 8, p. 1).

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 2016 L 119/1;

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018, on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union PE/53/2018/REV/1 *OJ L 303, 28.11.2018, p. 59–68;*

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), PE/86/2018/REV/1, *OJ L 151, 7.6.2019, p. 15–69,*

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), PE/86/2018/REV/1, *OJ L 151, 7.6.2019, p. 15–69,*

Recommendations and Guidelines:

AEPD (2019), Introduction to the hash function as a personal data pseudonymisation technique, Available at https://edps.europa.eu/sites/edp/files/publication/19-10-30_aepd-edps_paper_hash_final_en.pdf;

Article 29 Working Party (2005), "Working document on data protection issues related to RFID technology", WP 105, p.8. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2005/wp105_en.pdf;

Article 29 Working Party (2010), *Opinion 04/2007 on the Concept of Personal Data*,(WP 136) 01248/07/EN, p.10. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf;

Article 29 Working Party (2017), " Guidelines on the right to data portability", WP 242 rev.01, p.4 Available at: https://ec.europa.eu/newsroom/document.cfm?doc_id=44099;

Article 29 Working Party, Opinion 05/2014 on Anonymization Techniques, 0829/14/EN WP216, http://ec.europa.eu/justice/data-protection/ article-29/documentation/opinion-recommendation/files/2014/ wp216_en.pdf;

European Commission (2020), *Communication from the Commission to the European Parliament, The Council, The European Economic And Social Committee and The Committee of the regions, A European strategy for data, COM(2020)66 final*, Brussels;

European Commission (2020), Cybersecurity of 5G networks EU Toolbox of risk mitigating measures CG Publication; Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468;

Euroepan Commission Recommendation of Cybersecurity of 5G networks, C(2019) 2335 final. Available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=58154;

EDPB (2018), *The European Data Protection Board Endorsement 1/2018,* Available at: https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf;

EDPB (2019), ANNEX. Initial legal assessment of the impact of the U.S. CLOUD Act on the EU legal framework for the protection of personal data and the negotiations of an EU-US Agreement on cross-border access to electronic evidence,p.*3* Brussels. Available at: https://edpb.europa.eu/sites/default/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf;

EDPB (2020), Statement on the processing of personal data in the context of the COVID-19 outbreak.

EDPB (2021), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data Version 2.0;

EDPB (2021), Guidelines 07/2020 on the concepts of controller and processor in the GDPR Version 2.0.

International Legislation:

- Brazilian General Data Protection Law, Federal Law no. 13.709/2018 (or A *Lei Geral de Proteção de Dados* Pessoais (*LGPD*), Lei n° 13.709/2018);
- BVerfG, Urteil des Ersten Senats vom 15.Dezember1983- 1 BvR 209/83-,Rn.1-215;
- Children's Online Privacy Protection Act of 1998, 15 U.S.C. §§ 6501 – 6506;
- Clarifying Lawful Overseas Use of Data or CLOUD Act 18 U.S.C. §§2323,2713 (2018);
- Consumer Protection Code, Federal Law No. 8.078/90;
- Cybersecurity Law of the People's Republic of China No.53 (2016);
- Philippine Data Privacy Act of 2012 (Republic Act No. 10173);
- Data Security Law of the People's Republic of China No.84;
- E-Commerce Law of the People's Republic of China No.7 (2018);
- ECOWAS (2010), 'Supplementary Act on Personal Data Protection within ECOWAS',
- Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–2522 (2012);
- Fair Credit Reporting Act,12 U.S.C. §§1830-1831(1970) 15 U.S.C. §1681 et seq.(1970);
- False Identification Crime Control Act 18 U.S.C. § 1028(d)(7)(C) (2006);
- General Agreement on Trade in Services (1994), Marrakesh Agreement Establishing the World Trade Organisation, Annex 1B, 1869 U.N.T.S. 183, 33 I.L.M. 1167;

- Gesetz zum Schutz vor Missbrauch personenbezogener Daten bei der Datenverarbeitung (Bundesdatenschutzgesetz - BDSG), Bundesgesetzblatt Jahrgang 1977 Teil I Nr. 7, ausgegeben am 01.02.1977, Seite 201, 8.
- Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6809(4)(A);
- Health Information Technology for Economic and Health Act, Pub.L.No.111-5,123 Stat.226;
- Hesse Data Protection Act (1970) ["Hessisches Datenschutzgesetz 1970"] , Gesetzund Verordnungsblatt für das Land Hessen (HE GVBI), , nr. 41, Part I, p. 625-627;
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (Privacy Rules), THE GAZETTE OF INDIA [PART II-SEC. 3(i)];
- Indian Information Technology Act, 2000 (21 of 2000);
- Law"On Protection of Personal Data" of Ukraine, Official Bulletin of the Verkhovna Rada of Ukraine (BVR), 2010, No. 34, Art. 481. Available at:https://zakon.rada.gov.ua/laws/show/2297-17;
- League of Arab States. (2004). Arab Charter on Human Rights. League of Arab States, Article 16(8);
- Organisation of American States (1969), *American Convention on Human Rights, "Pact of San Jose", Costa Rica*, Article 11., available at: https://www.refworld.org/docid/3ae6b36510.html;
- Personal Information Protection Law of the People's Republic of China, No. 91(2021);
- Privacy Act, 5 U.S.C. § 552a (1974);
- Restatement (Second) of Torts, §652A (Am. Law Ins.1977);
- The California Consumer Act, A.B.375, 217 Gen Assemb., Reg. Sess. (Cal.2018);
- The Hacking Stop and Improving Electronic Data Security Act, S.B. 5775, Reg.Sess.2019-2020 (N.Y.2019);

- The Law on Personal Data Protection (Official Gazette of BIH', nos. 49/06, 76/11, and 89/11 or Zakon o zastiti licnih podataka ("Sl. glasnik BiH", broj 49/06, 76/11, and 89/11);
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996);
- Turkey's Personal Data Protection Law No. 6698 (2016), (Kişisel Verileri Koruma Kanunu - „KVKK");
- UN General Assembly (1966), *International Covenant on Civil and Political Rights*, United Nations, Treaty Series, vol. 999, p. 171, Article 17., available at: https://www.refworld.org/docid/3ae6b3aa0.html;
- UN General Assembly, Guidelines for the Regulation of Computerized Personal Data Files, 14 December 1990, available at: https://www.refworld.org/docid/3ddcafaac.html;
- UN General Assembly. (1948). *Universal declaration of human rights* (217 [III] A). Paris;
- UN General Assembly. (1948). *Universal declaration of human rights* (217 [III] A). Paris;
- Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (a)(3);

Case law:

- Benedik v. Slovenia, no. 62357/14, ECHR 2018;
- Bernh Larsen Holding AS and Others v. Norway, no. 24117/08, ECHR 2013;
- C 362/14 Maximillian Schrems v. Data Protection Commissioner [2015] ECLI:EU: C:2015:650;
- C-582/14: *Patrick Breyer v Bundesrepublik Deutschland*, ECLI:EU:C:2016:779;
- C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), EU:C:2011:771;
- Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González, ECLI:EU:C:2014:317;

- Case C-210/16, Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein against Wirtschaftsakademie Schleswig-Holstein GmbH ("Wirtschaftsakademie Schleswig-Holstein"), ECLI:EU:C:2018:388;
- Case C-25/17, *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta*, ECLI:EU:C:2018:551;
- Case C-40/17, *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, ECLI:EU:C:2019:629;
- Case C-673/17, *Planet49 GmbH v Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V.*, ECLI:EU:C:2019:801;
- Case Facebook Ireland and Schrems C-311/18, ECLI:EU:C:2020:559;
- Catt v. the United Kingdom, no. 43514/15, ECHR 2019, the ECtHR;
- G.S.B. v. Switzerland, no. 28601/11, ECHR 2015;
- Gaughran v. the United Kingdom, no. 45245/15, 13 ECHR 2020;
- Guillot v. France, no. 22500/93, ECHR 1996;
- I v. Finland ECHR (17 July 2008), application no. 20511/03;
- Joined Cases C-141/12 and C-372/12 YS [2014] EU: C:2014:2081, YS v Minister voor Immigratie, Integratie en Asiel, and Minister voor Immigratie, Integratie en Asiel v M and S;
- Katz v. United States, 389 U.S. 347 (1967);
- Patel vs Facebook Inc.No 18-15982,2019 WL 3727424, 9th Cir.Aug.8,2019;
- R.Österreich Datenschutzbehörde, Case: D155.027 2021-0.586.25;
- S. and Marper v. the United Kingdom, [GC], ECHR 2008;
- Sanchez v. Valencia Holding Co., 61 Cal. 4th 899 (2015);
- Schencke and Eifert v Hessen, Joined Cases C-92/09 and C-93/09 (9.11.2010), ECLI:EU:C:2010:662;
- Sorrell v. IMS Health Inc. 131 S. Ct. 2653 (2011);
- State v. Reid, 945 A.2d 26 (2008),194 N.J. 386;
- United States v. Microsoft Corp. (*Microsoft Ireland*), No. 17-2, slip op. at 3 (Apr. 17, 2018);
- Uzun v. Germany, no. 35623/05, ECHR 2010;
- Yershov v. Gannett Satellite Information Network, Inc., No. 15-1719;
- Z v. Finland, ECHR 1997, Reports of Judgments and Decisions 1997-I;

Agreements:

Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, USA No. 6 (2019); Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf;

Agreement for an Economic Partnership, EU-Japan, (2018), O.J. (L 330). Available at. http://publications.europa.eu/resource/cellar/d40c8f20-09a4-11e9-81b4-01aa75ed71a1.0006.01/DOC_1;

Argentina - Chile FTA (2017). Available at: https://edit.wti.org/document/show/bf9aa665-cb2a-472f-849d-090e28b096fb?textBlockId=834843bf-fbff-4d65-8829-67b41e122cf7&page=15;

Brazil - Chile FTA (2018). Available at: https://edit.wti.org/document/show/e62cfb4c-abbf-43d9-ae34-a15c7d057ab4;

Closer Economic Partnership Agreement between New Zealand and Singapore (2000), and upgraded in 2020 Available at: https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/nz-singapore-closer-economic-partnership/cep-text/#bookmark1 ;

Digital Economy Partnership Agreement (2020) Available at: https://www.mfat.govt.nz/assets/Trade-agreements/DEPA/DEPA-Signing-Text-11-June-2020-GMT-v3.pdf ;

EU-Armenia Comprehensive and Enhanced Partnership Agreement (2021). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:22018A0126(01);

FTA between the Government of the Republic of Korea and the Government of the Socialist Republic of Viet Nam (2015). Available at: https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/3582/download;

Government of Canada (2020) Agreement between Canada, U.S. and Mexico, Available at: https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/index.aspx?lang=eng;

The China–Australia Free Trade Agreement (2015). Available at: https://www.dfat.gov.au/trade/agreements/in-force/chafta/Pages/australia-china-fta;

The Singapore-Australia Free Trade Agreement (2003), and upgraded in 2021. Available at: https://www.dfat.gov.au/sites/default/files/agreement-to-amend-the-singapore-australia-free-trade-agreement.pdf;

U.S. – Jordan Free Trade Agreement (2001). Available at: https://ustr.gov/trade-agreements/free-trade-agreements/jordan-fta/final-text;

United States-Korea Free Trade Agreement (2012); Available at: https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text;

Books:

Atluri, V., & Pernul, G. (2014). *Data and Applications Security and Privacy XXVIII : 28th Annual IFIP WG 11.3 Working Conference, DBSec 2014, Vienna, Austria, July 14-16, 2014. Proceedings*. Springer Berlin Heidelberg;

Blum, D. (2020). *Rational Cybersecurity for Business : The Security Leaders' Guide to Business Alignment* (1st ed. 2020.). Apress Imprint: Apress;

Daradkeh, Y. I., & Mikhailovich, K. P. (2019). *Data sharing : : recent progress and remaining challenges*. Nova Science Publishers;

Kontargyris, X. (2018). *IT laws in the era of cloud-computing : a comparative analysis between EU and US law on the case study of data protection and privacy* (1. Auflage.). Nomos;

Kuşkonmaz, E. M. (2021). *Privacy and border controls in the fight against terrorism : : a fundamental rights analysis of passenger data sharing*. Brill | Nijhoff;

Lynn, T., Mooney, J. G., van der Werff, L., & Fox, G. (2021). *Data Privacy and Trust in Cloud Computing : Building trust in the cloud through assurance and accountability* (1st ed. 2021.). Springer International Publishing Imprint: Palgrave Macmillan;

Weber, R. H., Staiger, D., & Springer-Verlag GmbH Verlag. (2017). *Transatlantic data protection in practice* ([1st edition].). Springer;

Wiebe, A., & Dietrich, N. (2017). *Open Data Protection - Study on legal barriers to open data sharing - Data Protection and PSI*. Universitätsverlag Göttingen;

Articles and web sources:

Alan C. R. (2020),*" The Privacy, Data Protection and Cybersecurity Law Review"*, Sixth Edition, Available at: https://datamatters.sidley.com/wp-content/uploads/2019/11/The-Privacy-Data-Protection-and-Cybersecurity-Law-Review-Edition-6.pdf;

Anderson P.(1972), *Computer security technology planning study*. Technical Report ESD-TR-73-51, Volume 1, Available at: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande72a.pdf;

Ayre, L.B. and Craner, J. (2017) 'Open Data: What It Is and Why You Should Care', *Public library quarterly (New York, N.Y.)*, 36(2), pp. 173–184. Available at: https://www.tandfonline.com/doi/abs/10.1080/01616846.2017.1313045;

Bentotahewa, V., Hewage, C. & Williams, J. (2022), The Normative Power of the GDPR: A Case Study of Data Protection Laws of South Asian Countries. *SN COMPUT. SCI.* 3, 183; Available at: https://link.springer.com/article/10.1007/s42979-022-01079-z ;

Boeckl, K. and Lefkovitz, N. (2020), NIST Privacy Framework: A Tool for Improving Privacy Through Enterprise Risk Management, Version 1.0, Other, National Institute of Standards and Technology, Gaithersburg, MD, [online], Available at: https://doi.org/10.6028/NIST.CSWP.01162020;

Bradford, Anu. (2020) "*How the EU Became a Global Regulatory Power." In The Brussels Effect: How the European Union Rules the World*. New York: Oxford University Press. Oxford Scholarship Online, Available at: https://oxford.universitypressscholarship.com/view/10.1093/oso/9780190088583.001.0001/oso-9780190088583-chapter-2;

Burri, M. (2021) "*Data Flows and Global Trade Law*", Cambridge: Cambridge University Press, pp. 11–41. Available at: https://www.cambridge.org/core/books/big-data-

and-global-trade-law/data-flows-and-global-trade-law/E98D121FC172A9F534DE9C310919E389;

Cate, Fred H.; Cullen, P.; and Mayer-Schonberger, V. (2013), "Data Protection Principles for the 21st Century" . *Books & Book Chapters by Maurer Faculty*. Available at: https://www.repository.law.indiana.edu/facbooks/23;

Chander, Anupam and Le, Uyen P.(2014), *Breaking the Web: Data Localization vs. the Global Internet*, Emory Law Journal, Forthcoming, UC Davis Legal Studies Research Paper No. 378,. Available at: SSRN: https://ssrn.com/abstract=2407858;

Christakis T., (2020) *"'European Digital Sovereignty': Successfully Navigating Between the "Brussels Effect" and Europe's Quest for Strategic Autonomy'*, Multidisciplinary Institute on Artificial Intelligence/Grenoble Alpes Data Institute, e-book, Available at https://ssrn.com/abstract=3748098 & https://airegulation.com;

Cory N., Dascoli L., (2021), "How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them" (ITIF, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost**;**

Cory, N. (2017). *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*.ITIF, P.4. Available at: https://www.researchgate.net/publication/333292633_Cross-Border_Data_Flows_Where_Are_the_Barriers_and_What_Do_They_Cost;

CPA (2020), "*Implementing Data Portability: Lessons for a Made-In-Canada Approach*", Available at: https://www.cpacanada.ca/en/public-interest/public-policy-government-relations/policy-advocacy/data-governance/data-portability;

Curry, Zillner, S., Metzger, A., Pazzaglia, J.-C., & Robles, A. G. (2021). *The Elements of Big Data Value: Foundations of the Research and Innovation Ecosystem*. National University of Ireland; Available at: https://link.springer.com/book/10.1007/978-3-030-68176-0;

Daskal, J. (n.d.). The Opening Salvo: The CLOUD Act, e-Evidence Proposals, and EU–US Discussions Regarding Law Enforcement Access to Data across Borders. In (pp. 319-341). doi:10.1017/9781108755641.012;

De La Chapelle B. and Porciuncula L (2021). *We Need to Talk About Data: Framing the Debate Around the Free Flow of Data and Data Sovereignty*. Internet & Jurisdiction Policy Network (I&JPN), Paris. Available at: https://www.internetjurisdiction.net/news/aboutdata-report;

Doldirina, C., Eisenstadt, A., Onsrud, H., & Uhlir, P. (2018). *Legal Approaches for Open Access to Research Data*,.Available at: https://doi.org/10.31228/osf.io/n7gfa;

Doneda D.(2022), Guidelines for judicial actors on privacy and data protection, UNESCO, Available at: https://unesdoc.unesco.org/ark:/48223/pf0000381298;

Edelstein, Michael & Sane, Jussi. (2015). *Overcoming Barriers to Data Sharing in Public Health: A Global Perspective*., Available at: https://www.chathamhouse.org/sites/default/files/field/field_document/20150417OvercomingBarriersDataSharingPublicHealthSaneEdelstein.pdf

European Commission, Directorate-General for the Information Society and Media, Carrara, W., Fischer, S., Steenbergen, E., et al. (2017) *Creating value through open data: a study on the impact of re-use of public data resources*. Publications Office, Available at: https://data.europa.eu/doi/10.2759/328101;

Ferracane, M.F. (2019), "*Data flows and national security: a conceptual framework to assess restrictions on data flows under GATS security exception*", Digital Policy, Regulation and Governance, Vol. 21 No. 1, pp. 44-70, Available at: https://doi.org/10.1108/DPRG-09-2018-0052;

Finck, M. and Pallas, F. (2020) '*They who must not be identified—distinguishing personal from non-personal data under the GDPR*', International data privacy law, 10(1), pp. 11–36. Available at: https://academic.oup.com/idpl/article/10/1/11/5802594.;

Fraser e.,(2016) "Data Localisation and the Balkanisation of the Internet," *SCRIPTed*, Vol. 13, p. 359, https://script-ed.org/article/data-localisation-and-the-balkanisation-of-the-internet/;

AICPA and CICA, (2009), Generally Accepted Privacy Principles, Available at: https://bcourses.berkeley.edu/courses/1457298/files/70759534/download?verifier=k75et0haGLJqYtVlHNos0BiXVLdNOOEIjNCL2zBG&wrap=1;

Hartzog, W. (2017) 'The inadequate, invaluable fair information practices,' *Maryland law review (1936)*, 76(4),. Available at:

https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3017312_code1107005.pdf?abstractid=3017312&mirid=1;

HODSON, S. (2019) "Applying WTO and FTA Disciplines to Data Localization Measures," World Trade Review. Cambridge University Press, 18(4), pp. 579–607. Available at: https://doi.org/10.1017/S1474745618000277;

Information Commissioner's Office (2012), '*Anonymisation: Managing Data Protection Risk Code of Practice*', Available at: https://ico.org.uk/media/1061/anonymisation-code.pdf;

Kapoor, A., and Amrita N. (2021),"Non-Personal Data Sharing: Potential, Pathways and Problems." *CSI Transactions on ICT*, vol. 9, no. 3, Springer India, pp. 165–169, https://doi.org/10.1007/s40012-021-00336-5;

Korn N.(2010), *Overview of the 'Openness' of Licences to Provide Access to Materials, Data, Databases and Media,* JISC Legal, Available at: http://sca.jiscinvolve.org/wp/files/2010/12/SCA_BP_Open_Licences_Dec10_v1-02.pdf;

Lee, Jyh-*An (2017), Licensing Open Government Data* , Hastings Business Law Journal, Vol. 13, No. 2, , The Chinese University of Hong Kong Faculty of Law Research Paper 2017-07, Available at SSRN: https://ssrn.com/abstract=2964704;

Lowrance, W. W. (2012) "Identifiability and person-specific data," in Privacy, Confidentiality, and Health Research. Cambridge: Cambridge University Press (Cambridge Bioethics and Law), pp. 87–110. Available at: https://doi.org/10.1017/CBO9781139107969.008;

McCullagh, K. (2017), *Data Sensitivity: Proposals for Resolving the Conundrum. Journal of International Commercial Law and Technology*, Vol. 2, Issue 4, pp. 190-201, Available at SSRN: https://ssrn.com/abstract=1378121;

McIntyre, J.J. (2011) „*Balancing expectations of online privacy: why Internet Protocol addresses should be protected as personally identifiable information*", *The De Paul law review*, 60(3), Available at: https://via.library.depaul.edu/cgi/viewcontent.cgi?article=1151&context=law-review;

Mitchell, A. D. and Hepburn, J. (2017), *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer*. 19 Yale Journal of Law and Technology 182, Available at SSRN: https://ssrn.com/abstract=2846830;

Molinuevo,M. And Gaillard,S. J. H.(2018) *Trade, Cross-Border Data, and the Next Regulatory Frontier : Law Enforcement and Data Localization Requirements (English)*. MTI Practice Note,no. 3 Washington, D.C. : World Bank Group.. Available at: http://documents.worldbank.org/curated/en/903261543589829872/Trade-Cross-Border-Data-and-the-Next-Regulatory-Frontier-Law-Enforcement-and-Data-Localization-Requirements;

Monino, J.-L. and Sedkaoui, S. (2016) *Big data, open data and data development*. 1st edition. Hoboken, New Jersey :: ISTE Ltd/John Wiley and Sons Inc. Available at: https://onlinelibrary-wiley-com.uaccess.univie.ac.at/doi/book/10.1002/9781119285199;

National Research Council (2012), *For Attribution: Developing Data Attribution and Citation Practices and Standards: Summary of an International Workshop*. Washington, DC: The National Academies Press. https://doi.org/10.17226/13564;

NIST (2015), *Privacy Risk Management for Federal Information Systems, National Institute of Standards and Technology Internal Report 8053*, Washington, DC,Available at http://dx.doi.org/10.6028/NIST.IR.8053;

OECD (2002) *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD Publishing. Available at: https://doi.org/10.1787/9789264196391-en.

OECD (2002), *Mapping approaches to data and data flows - Report for the G20 Digital Economy Task Force*. Paris: OECD Publishing, Available at: https://www.oecd.org/sti/mapping-approaches-to-data-and-data-flows.pdf;

OECD (2014), Summary of OECD Expert Roundtable: "*Protecting Privacy in a Data-driven Economy: Taking Stock of Current Thinking*", OECD, Paris, Available at: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=dsti/iccp/reg%282014%293&doclanguage=en;

OECD (2020), *OECD Digital Economy Outlook 2020*, OECD Publishing, Paris, Available at: https://doi.org/10.1787/bb167041-en;

OECD (2021), Data Portability, Interoperability and Digital Platform Competition, OECD Publishing, Paris, Available at: https://www.oecd.org/daf/competition/data-portability-interoperability-and-digital-platform-competition-2021.pdf;

Pagliari, C., Davidson, S., Cunningham-Burley, S., Laurie, G., Aitken, M., Sethi, N. (2013). *Public Acceptability of Data Sharing Between the Public, Private and Third Sectors for Research Purposes.* Scottish Government Social Research, available at: https://www.researchgate.net/publication/257963356_Public_Acceptability_of_Data_Sharing_Between_the_Public_Private_and_Third_Sectors_for_Research_Purposes;

Papakonstantinou, V. & Hert, P.. (2015). *The Data Protection Regime in China. In-Depth Analysis*, Brussels Privacy Hub Working Paper, Volume 1, Number 4, Available at: SSRN: https://ssrn.com/abstract=2773577 ;

Phillips, M.(2018), *International data-sharing norms: from the OECD to the General Data Protection Regulation (GDPR)*. *Hum Genet* 137, 575–582 (2018). Available at: https://doi.org/10.1007/s00439-018-1919-7;

Podda, E. and Palmirani, M. (2021) 'Inferring the Meaning of Non-personal, Anonymized, and Anonymous Data', in *AI Approaches to the Complexity of Legal Systems XI-XII*. Cham: Springer International Publishing, pp. 269–282.; https://link.springer.com/chapter/10.1007/978-3-030-89811-3_19;

Purtova, N. (2010) '*Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights'*, Netherlands quarterly of human rights, 28(2), pp. 179–198.. Available at: https://www.researchgate.net/publication/228147350_Private_Law_Solutions_in_European_Data_Protection_Relationship_to_Privacy_and_Waiver_of_Data_Protection_Rights;

R.D. Kush, D. Warzel, M.A. Kush, A. Sherman, E.A. Navarro, R. Fitzmartin, F. Pétavy, J. Galvez, L.B. Becnel, F.L. Zhou, N. Harmon, B. Jauregui, T. Jackson, L. Hudson (2020*), FAIR data sharing: The roles of common data elements and harmonization*,

Journal of Biomedical Informatics, Volume 107, ISSN 1532-0464,; Available at: https://doi.org/10.1016/j.jbi.2020.103421;

Raul,A.C. (2014), The Privacy, Data Protection and Cybersecurity Law Review, Law Business Research Ltd, London,. Available at: https://www.sidley.com/~/media/files/publications/2014/11/the-privacy-data-protection-and-cybersecurity-la__/files/apec-overview/fileattachment/apec-overview.pdf;

Rich C., "A Look at New Trends in 2017: Privacy Laws in Europe and Eurasia (non-EEA)," (Bloomberg Law, July 17, 2017), Available at: https://media2.mofo.com/documents/170717-privacy-lawseurope-eurasia.pdf;

Samarati, P. and de Vimercati, S.C. (2001) '*Access Control: Policies, Models, and Mechanisms*', in *Foundations of Security Analysis and Design*. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 137–196. Available at: https://link.springer.com/chapter/10.1007/3-540-45608-2_3;

Schwalbe N., Wahl B., Song J., Lehtimaki S.(2020), *Data Sharing and Global Public Health: Defining What We Mean by Data,* Frontiers in Digital Health, VOLUME 2, Available at: https://www.frontiersin.org/article/10.3389/fdgth.2020.612339;

Simpson E., Brown R., Sillence E., Coventry L., Lloyd K., Gibbs J., Tariq Sh.a, Durrant A.(2021), *Understanding the Barriers and Facilitators to Sharing Patient-Generated Health Data Using Digital Technology for People Living With Long-Term Health Conditions: A Narrative Review* , Frontiers in Public Health, Volume 9, Available at: URL=https://www.frontiersin.org/article/10.3389/fpubh.2021.641424;

Soprana, M.(2021). *The Digital Economy Partnership Agreement (DEPA): Assessing the Significance of the New Trade Agreement on the Block*. Trade, Law and Development. XIII. 143. Available at: https://www.researchgate.net/publication/354472706_The_Digital_Economy_Partnership_Agreement_DEPA_Assessing_the_Significance_of_the_New_Trade_Agreement_on_the_Block;

Staunton, C.(2021): *Data Sharing and the Public Interest in a Digital Pandemic*,* p.2. *Available at: VerfBlog,* Available at: https://verfassungsblog.de/data-sharing-and-the-public-interest-in-a-digital-pandemic/;

Taylor, R.D. (2020) '"Data localization": The internet in the balance', *Telecommunications policy*, 44(8),Available at: https://www.sciencedirect.com/science/article/pii/S0308596120300951;

UNCTAD (2021), *Digital Economy Report - Cross-border data flows and development: For whom the data flow*, United Nations Publications, Available at: https://unctad.org/webflyer/digital-economy-report-2021;

US Department of Health, Educ. & Welfare, (1973), *Records, Computers And The Rights Of Citizens: Report Of The Secretary's Advisory Committee on Automated Personal Data Systems*, no. (Os)73-94, Available at: https://www.justice.gov/opcl/docs/rec-com-rights.pdf;

Van Alsenoy, B., 2016. *Regulating data protection: the allocation of responsibility and risk among actors involved in personal data processing*, p.293. Available at: https://www.researchgate.net/publication/308201270_Regulating_data_protection_the_allocation_of_responsibility_and_risk_among_actors_involved_in_personal_data_processing;

van den Hoven, Jeroen, Martijn Blaauw, Wolter Pieters, and Martijn Warnier, Edward N. Zalta (ed.) (2020) "Privacy and Information Technology", *The Stanford Encyclopedia of Philosophy* , Available at: https://plato.stanford.edu/entries/it-privacy/;

Wessels, B. *et al.* (2017) *Open Data and the Knowledge Society*. Amsterdam: Amsterdam University Press. Available at: https://library.oapen.org/bitstream/handle/20.500.12657/31743/625332.pdf?sequence=1&isAllowed=y;

Wong J., Henderson T. (2019), *The right to data portability in practice: exploring the implications of the technologically neutral GDPR*, *International Data Privacy Law*, Volume 9, Issue 3, Pages 173–191, Available at: https://doi.org/10.1093/idpl/ipz008;

World Economic Forum,(2019), *The Next Generation of Data-Sharing in Financial Services: Using Privacy Enhancing Techniques to Unlock New Value (White Paper)*, Available at: https://www3.weforum.org/docs/WEF_Next_Gen_Data_Sharing_Financial_Services.pdf;

Yakovleva, S. (2018) "*Should Fundamental Rights to Privacy and Data Protection be a Part of the EU's International Trade 'Deals'?,*" World Trade Review. Cambridge University Press, 17(3), pp. 477–508. Available at: DOI: https://doi.org/10.1017/S1474745617000453,

Zachariadis M.(2020), *"Data-sharing frameworks in financial services: Discussing open banking regulation for Canada"* Available at: SSRN: https://ssrn.com/abstract=2983066 ;