The EU General Data Protection Regulation (GDPR): Five Years After and the Future of Data Privacy Protection in Review ©

Alexander A Wodi[1]

Abstract

The General Data Protection Regulation (GDPR), which came into effect in 2018, is one of the most advanced and recognizable international pieces of legislation for data privacy and protection. Since its inception, the GDPR has elevated data privacy and protection in stature within the EU and globally. The GDPR has local and extra-territorial applications. It applies to the EU and its residents as well as foreign and EU companies engaged in the processing or international transfer of the personal data of EU citizens to and from the EEA.

Following the passage of the GDPR many countries' data protection laws have been modeled after the innovative EU Statute at the national and subnational level (Brazil – LGPD, Canada – PIPEDA, Nigeria – NDPA, and California – CPRA). There has been increased awareness about individual privacy rights. There have also been big fines and penalties against companies in the social media and e-Commerce space for noncompliance with GDPR principles (e.g., Facebook – 1.2 bn Euros and Amazon – 746 m euros). In this paper we examine the successes and challenges of five years of GDPR and take a snapshot of what the future holds for the groundbreaking legislation; and the data privacy and security continuum.

We shall also examine, *inter alia*, the guiding principles of the GDPR *vis-à-vis* the collection, use, retention, and disclosure of personal data; the obligations of data controllers and data processors in respect of the handling and processing of data; the rights of data subjects; International data transfers and data flows; Adequacy Decisions; the use of BCRs and SCCs for data transfers; derogations for specific situations; the Safe Harbor Program and Privacy Shield; Schrems I and II; the new EU-US Data Privacy Framework; Privacy by Design (PbD); Data Protection Impact Assessment (DPIA); Privacy Enhancing Technologies (PET); and Enforcement Actions by Data Protection Authorities (DPAs) in the EU; Data localisation; AI Governance; and Web 3.0.

Key Words: General Data Protection Regulation (GDPR); Data Privacy; International Data Transfer; Schrems I and II; and EU-US Data Privacy Framework.

---

[1] Alex Wodi (JD/LLB, BL, LLM, CIPP/US, ACIArb, UK, Member ICMC) is a lawyer and a certified data privacy professional, CIPP/US. He has a background in banking and commercial law, regulatory compliance, international law, and comparative law. He is also a chartered arbitrator, mediator, and conciliator. He has written many scholarly articles and is the author of *Garnishment Law and Practice in Nigeria, UK, and US* (Amazon, and Barnes & Noble, 2023) ISBN 9798987288306 and *The Most Expensive Real Estate and Other Works: An Anthology of Essays, Poems and Artworks on the Cusp of a Pandemic* (Amazon, 2021) ISBN 9798706781880. He may be contacted via email – aawodi21@yahoo.com, or alexwodi@wodiandwodi.com.

Contents

1.0 EU Data Protection Law: GDPR

The European Union (EU)'s General Data Protection Regulation (GDPR) is perhaps the strictest and most advanced privacy and security law in the world.[1] The GDPR came into force on 25 May 2018, and it applies to foreign and EU companies that collect, or process data connected to EU data subjects.[2]

Prior to the GDPR, the EU passed the European Data Protection Directive in 1995,[3] which provided minimum standards of data privacy and protection. Guided by the Directive EU member states passed their individual implementing laws. With the expansion of the internet, and growth of the digital economy, data became one of the primary resources utilized by companies, search engines, social networks, and platforms. In 1994, the first banner ad appeared online. In 2000, a majority of financial institutions offered online banking. In 2006, Facebook opened to the public allowing persons 13 years and older to register and open an account.[4] The 2011, lawsuit against Google by a consumer for unauthorized scanning of her email[5] spurred the European data

[1] It may be argued that the California law, the CCPA (as amended by CPRA), which was modelled after the GDPR, is also a contender for the title.

[2] The GDPR is recognised as the gold standard for data privacy and security. Many countries (especially commonwealth nations, e.g., Brazil, Canada, India, and Nigeria) have modelled their data protection and privacy laws after the GDPR. This is not unconnected with the Brussels Effect (which is the process of unilateral regulatory globalisation caused by the European Union *de facto* (but not necessarily *de jure*) externalising its laws outside its borders through market mechanisms.) The *Brussels effect* and *California effect* are a form of "race to the top" where the most stringent standard has an appeal to companies operating across multiple regulatory environments as it makes global production and exports easier. cf. the *Delaware effect*, a race to the bottom where jurisdictions can purposefully choose to lower their regulatory requirements in an attempt to attract businesses looking for the least stringent standard. See David Bach, "Three Questions: Prof. David Bach on the Reach of European Privacy Regulations" (*Yale Insight*, 25 May 2018) <https://insights.som.yale.edu/insights/three-questions-prof-david-bach-on-the-reach-of-european-privacy-regulations> accessed 2 October 2023.

[3] EUR-Lex, "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" (*EU Website*, 20 November 2003) < https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046> accessed 27 September 2023.

[4] GDPR Info Page, "History of the GDPR" Regulation (EU) 2016/679 (General Data Protection Regulation) of the European Parliament and of the Council of 27 April 2016 in the current version of the OJ L 119, 4.5.2016 <https://gdprinfo.eu/what-is-gdpr-the-eus-new-data-protection-law> accessed 3 October 2023.

[5] *Marquis v. Google, Inc.*, No. SUCV2011-02808-BLS1 (Mass. Super. Jun. 27, 2014). See also Warwick Ashford, "US Woman Sues Google Over Gmail Scanning" (*Computer Weekly*, 11 August 2011) <https://www.computerweekly.com/news/2240105327/US-woman-sues-Google-over-Gmail-scanning> accessed 2 October 2023. cf, Similar lawsuit before a US district court sitting in San Jose, California against google for violation of federal and state wiretap laws through unlawful data mining practices involving the unauthorized scanning of Gmail accounts for alleged targeted advertising. See B Herold, "Google Under Fire for Data Mining Student Email Messages" (*Education Week*, 13 March 2014) < https://www.edweek.org/policy-politics/google-under-fire-for-data-mining-student-email-messages/2014/03> accessed 2 October 2023.

protection supervisor (EDPS) to begin work on the amendment of the 1995 directive.[6] The EDPS declared that the EU needed "a comprehensive approach on personal data protection."[7]

The European Parliament approved the GDPR in 2016 and by 25 May 2018, all companies and organisations involved in processing personal data of EU data subjects were required to be compliant. The GDPR provides a strict two-tier regime of penalties for violations:

i. **The High-level category** focuses on infringements related to the basic principles of processing (including consent, lawfulness, and processing sensitive data), international transfers of personal data, and rights of data subjects. The maximum fines under this category are the greater of €20 million or 4% of global annual revenue.[8]
ii. **The lower-level category** includes such infringements as failure to integrate data privacy by default or design, record keeping, security of data, designation of DPO, communication of data breach notification to DPAs and data subjects,[9] or lack of cooperation with DPAs. In this category the maximum fines are €10 million or 2 % global annual revenue (whichever is higher).[10]
iii. Data subjects also have the right to sue and seek compensation for damages.[11]

1.1. GDPR Definitions and Principles

Article 4 of the GDPR defines data subjects; data controllers, data processors and personal data as follows:

- **'data subject'** means *an identified or identifiable natural person. An individual to whom personal data relates.*
- **'data controller'** means *the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.*
- **'data processor'** means *a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.*
- **'personal data'** means *any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly*

[6] GDPR Info Page, "History of the GDPR" ibid.
[7] EDPS (Official website of EU) <https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en> accessed 2 October 2023.
[8] art 83(5) and (6) GDPR.
[9] art 33 GDPR requires data breach notification to be without undue delay, where feasible within 72 hours of becoming aware of the breach.
[10] art 83(4) GDPR.
[11] arts 79 and 82 GDPR.

or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

Article 9 of the GDPR defines '**special categories of personal data'** or **'sensitive personal information'** as:

- *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*.

Processing of sensitive personal data is prohibited unless with the express consent of the data subject and for certain specified purposes.[12]

Article 5 of the GDPR stipulates **seven guiding principles** for processing personal data, which are similar to the OECD framework for Fair Information Principles (FIPs).[13] These include:

i. *Lawfulness, fairness, and transparency* — There must be a legal basis for processing of data which is expected to be in a fair, and transparent manner. Data collection and processing must be with the consent of the data subject and in compliance with GDPR principles and requirements.
ii. *Purpose limitation* — The processing of data must be limited to the intended and specified purposes Data must be processed for the legitimate purposes expressly specified to the data subject at the time of collection or immediately thereafter.
iii. *Data minimization* — Only the data required or absolutely necessary for the purposes specified should be collected and processed.
iv. *Accuracy* — The personal data must be accurate and kept up to date.
v. *Storage limitation* — Personally identifying data can only be stored for as long as necessary for the specified purpose.
vi. *Integrity and confidentiality* — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g., by using encryption).
vii. *Accountability* — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles. These include documenting and reporting data breaches, maintaining a record of processing activities and conducting DPIAs.[14]

[12] art 9 GDPR.
[13] Also known as fair information privacy practices or principles (FIPPs).
[14] See arts 30, 33 and 35 GDPR.

1.2 Data Subjects Rights

Data Subjects have the following **privacy rights** under the GDPR –

- *right to be informed*[15] – Controllers have to notify data subjects when they fulfill requests for erasure, rectification, or restriction of processing.
- *right of access*[16] – Data subjects have the right to know what data are collected and why, to know how their data will be processed and with whom their data may be shared, and to obtain a copy of their personal data as well as information about how to request erasure under GDPR.[17]
- *right to rectification*[18] – Data subjects have the right to request corrections of inaccurate outdated information collected about them.
- *right to erasure*[19] - This is better known as the right to be forgotten. After receiving this request, controllers are required to erase the personal data in question without any undue delay. After receiving a request to be forgotten, a data controller or processor can only retain personal data as required to meet other legal obligations.
- *right to restrict processing*[20] – Data subjects have the right to request that controllers halt processing activities, without requesting full erasure, in some circumstances.
- *right to data portability*[21] - Subjects have the right to get a copy of their data in machine readable format so that it can be brought into other information systems. This right helps prevent companies from locking customers into their products by keeping data in a proprietary format that cannot be moved to a competing system.
- *right to object*[22] - Data subjects have the right to object to any processing of their personal data that they believe is out of compliance with GDPR, and they have the right to opt out of certain data processing activities such as direct marketing. The onus is on the data controller to demonstrate that data processing activities are authorized under GDPR in order to resume. Data subjects also have the right to withdraw previously given consent.[23]
- *rights in relation to automated decision-making and profiling*[24] - This means that artificial intelligence, or any automated processing alone cannot make decisions that have a significant or legal impact on a person if the person opts out of that decision-making.

---

[15] art 12 -14 GDPR.
[16] art 15 GDPR.
[17] Most of these details now form part of the standard format for organization's privacy notices. the GDPR now empower individuals to file a data subject request (DSR). By filing a DSR the data subject has a right to access, correct, restrict, or erasure of his personal data. A Data Subject Access Request (DSAR) on the other hand is a specific request for access to the data subjects personal data. the DSAR is part of a larger umbrella term, i.e., DSR.
[18] art 16 GDPR.
[19] art 17 GDPR.
[20] art 18 GDPR.
[21] art 20 GDPR.
[22] art 21 GDPR.
[23] art 7 GDPR.
[24] art 22 GDPR.

It is important to note that upon examination all the data subject rights are correlated and based on the seven GDPR guiding principles from which they find imprimatur. There are also strict rules regarding consent and processing of personal data. Data can only be processed upon data subject's consent which must be "freely given, specific, informed and unambiguous." The GDPR requires opt in consent which is explicit and affirmative.[25] The GDPR has fostered increased awareness of data privacy rights by individuals globally since 2018, and it should continue to expand into the future with the passage of data protection laws by more countries.[26]

2.0 International Transfers and Data flows

GDPR allows transfers between member states, but it requires that organizations follow a process before transferring data outside of the European Union. There are three major ways this can be done.

Firstly, organizations can adopt a set of **standard contractual clauses** (SCCs) that have been approved for use in data transfers outside of the EU.[27] Samples of these clauses are available on the EU's website,[28] and may be adopted and integrated into contracts.

Secondly, organizations may adopt **binding corporate rules** (BCRs) that regulate data transfers.[29] BCRs are a time-consuming process as the rules must be approved by every EU member nation where they will be used and undergo rigorous review by the EU member state supervisory authority. This route is, therefore, typically only adopted by very large organizations.

Finally, prior to Schrems I, the European Union, and the United States operated a safe harbor program. Organizations could certify their compliance with privacy practices through an independent assessment, and if they passed, were permitted to transfer information. The safe harbor program was struck down by the European Court of Justice in Schrems I[30] in 2015. In 2016

---

[25] The GDPR defines 'consent' of the data subject to mean *any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*

[26] Gartner, "Gartner Identifies Top Five Trends in Privacy Through 2024" (Stamford, Conn., 31 May 2022) < https://www.gartner.com/en/newsroom/press-releases/2022-05-31-gartner-identifies-top-five-trends-in-privacy-through2024#:~:text=%E2%80%9CBy%20year%2Dend%202024%2C%20Gartner%20predicts%20that%2075%25%20of%20the%20world%E2%80%99s%20population%20will%20have%20its%20personal%20data%20covered%20under%20modern%20privacy%20regulations.> accessed 5 September 2023.

[27] arts 46 and 93 GDPR.

[28] EU Standard Contract Clauses - <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en> accessed 19 September 2023.

[29] art 47 GDPR.

[30] *Schrems v. Data Protection Commission* (C-362/14) EU:C: 2015:650, October 6, 2015, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362> accessed 17 September 2023. The decision was largely based on concerns raised by the Edward Snowden revelations about US government surveillance in 2013. Since a 1995 EU directive/law, personal data may generally not be sent outside of the EU unless there is "essentially equivalent" protection in the destination country. The US heavily relied on the European Commission decision under

the US-EU Safe Habor was replaced by an agreement called Privacy Shield.[31] However, a 16 July 2020 ruling by the European Court of Justice in another case called Schrems II[32] declared that the EU-US Privacy Shield was invalid.[33] So companies could not rely on the Privacy Shield and resorted to using either SCCs or BCRs.[34]

Following further negotiations between the US and EU authorities, on 10 July 2023, the European Commission adopted its **adequacy decision** for the EU-U.S. Data Privacy Framework. The adequacy decision concluded that the United States ensures an adequate level of protection – compared to that of the EU - for personal data transferred from the EU to US companies participating in the EU-U.S. Data Privacy Framework.[35]

An adequacy decision is one of the tools provided under the General Data Protection Regulation (GDPR) to transfer personal data from the EU to third countries which, in the assessment of the Commission, offer a comparable level of protection of personal data to that of the European Union.[36] Where a transfer is not covered by an adequacy decision or appropriate safeguards, the GDPR provides **derogations**[37] (or exceptions) under which a transfer may take place. The derogations permit a transfer where the data subject has given explicit consent or if the transfer is necessary for:

- Performance of a contract between the data subject and the data controller;
- to conclude a contract in the interest of the data subject between a controller and third party;
- important reasons of public interest;

---

the "Safe Harbor Program" that declared the US "essentially equivalent" in 2000. The CJEU annulled the Commission Decision in C-362/14 ("Schrems I") in 2015, given the invasive US surveillance laws (US Patriot Act; FISA 702; and EO 12.333).

[31] In 2016 the European Commission passed largely the same Decision on EU-US Data Transfers again, under the new name "Privacy Shield" which was invalidated by the CJEU in C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited, Maximilian Schrems* ("Schrems II") in 2020 largely on the same grounds.

[32] Ibid. C-311/18, *Data Protection Commissioner v. Facebook Ireland Limited, Maximilian Schrems* (Schrems II).

[33] The cases were brought before the CJEU by Max Schrems, an Austrian privacy advocate, founder of NYOB. Both cases are known and referred to as "Schrems I and II" after the complainant.

[34] Although the supplemental measures and modifications made to SCC by companies such as Meta's Facebook have been held to be inadequate resulting in record 1.2 billion euros GDPR fines. They do not appear to compensate for the deficiencies in the US law identified by the CJEU in the Schrems II judgment, absent an adequacy decision. Thus, data exporters who make extra-EEA transfers must implement measures that ensure essential equivalence to EU data protection standards in the recipient country.

[35] Twenty-four EU member states — representing a population of more than 424 million — voted on 7 July 2023 in favor of the EU-US Data Privacy Framework while three unnamed member states abstained.

[36] art 44-46 GDPR. List of Adequate states/countries as at January 2023 -
• Andorra • Argentina • Canada (partial) • EU, EEA • Faroe Islands • Gibraltar • Guernsey• Iceland • Isle of Man
• Israel • Japan (partial) • Jersey• Liechtenstein • New Zealand • Norway • South Korea • Switzerland • Uruguay
No additional transfer mechanism is required where data is being transferred from the EU / UK to any of these adequate states. EU GDPR Adequacy decisions are based on *Essential Equivalence* – safeguards, rights, remedies in the recipient state must be 'essentially equivalent' to those provided in EU.

[37] art 49 GDPR

- Exercise or defense of a legal claim or right; protection of the interest of an individual incapable of giving consent;
- and a compelling legitimate interest subject to compliance with GDPR requirements, including notice to the DPA of the transfer.[38]

As a result of adequacy decisions, personal data can flow freely and safely from the European Economic Area (EEA), which includes the 27 EU Member States as well as Norway, Iceland, and Liechtenstein, to a third country, without being subject to any further conditions or authorisations. In other words, transfers to the third country can be handled in the same way as intra-EU transmissions of data.

The adequacy decision on the EU-U.S. Data Privacy Framework covers data transfers from any public or private entity in the EEA to US companies participating in the EU-U.S. Data Privacy Framework.[39]

2.1 EU-U.S. Data Privacy Framework

The much-anticipated adequacy decision on the EU-US data privacy framework post Schrems II invalidation of the EU-US privacy shield was approved on 7 July 2023 by a majority vote of 24 EU member states.[40] A press release published by the European Commission said the "EU-U.S. Data Privacy Framework introduces new binding safeguards to address all the concerns raised by the European Court of Justice, including limiting access to EU data by U.S. intelligence services to what is necessary and proportionate and establishing a Data Protection Review Court."[41]

- *Necessary and Proportionate* - the framework "clearly" spells out necessity and proportionality requirements and "enforceable safeguards" with a "user friendly" redress mechanism. Access to data is limited to what is necessary and proportionate to protect national security.
- *Data Protection Review Court* - EU individuals will have access to an independent and impartial redress mechanism regarding the collection and use of their data by US intelligence agencies, which includes a newly created Data Protection Review Court (DPRC). The DPRC will have the power to order deletion of data if it is found to be collected in violation of the new safeguards.
- *Qualifying States* - Under the U.S. commitments, EU member states along with Iceland, Liechtenstein and Norway are "qualifying states," and citizens will be able to file for

[38] Ibid.
[39] EU FAQ about EU-US Privacy Framework agreed in July 2023. See also (on international data transfers) Mike Chapple, ibid 228 – 231; and P Swire an DK Mayo, *US Private-Sector Privacy: Law and Practice for Information Privacy Professionals,* (3rd edn, An IAPP Publication 2020) 407 – 408.
[40] Jennifer Bryant, "European Commission adopts EU-US adequacy decision" (*IAPP,* 10 July 2023) < https://iapp.org/news/a/european-commission-adopts-eu-u-s-adequacy-decision/ > accessed 12 July 2023.
[41] Press Release, 10 July 2023, EU, < https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721 > accessed 12 July 2023

redress through the Data Protection Review Court while obtaining enhanced U.S. privacy protections.

- *Scope and Applicability* – The safeguards put in place by the EU-US DPF will also apply when data is transferred by using other tools, such as standard contractual clauses and binding corporate rules.
- *Periodic Review* - The functioning of the EU-U.S. Data Privacy Framework will be subject to periodic reviews, to be carried out by the European Commission, together with representatives of European data protection authorities and competent US authorities.[42]

2.2 Why there may be a Schrems III.

The IAPP provides an apt background on Schrems and his groundbreaking cases –

> "… Maximilian Schrems first came to notoriety as an Austrian law student, who filed a complaint with the Irish Data Commissioner against Facebook Ireland for illegally sharing his personal data with the U.S. government, following the revelations of Edward Snowden. The case, known as 'The Schrems case' or 'Schrems I,' eventually led to the invalidation of the Safe Harbor data-transfer agreement between the EU and U.S. ('Safe Harbor' and 'Privacy Shield'). Schrems later amended his complaint against Facebook Ireland with the Irish Data Protection Commission after Facebook switched its transfer mechanism from Safe Harbor to standard contractual clauses, leading to a new referral to the CJEU implicating both standard contractual clauses and the EU-U.S. Privacy Shield Framework. On July 16, 2020, the Court of Justice of the European Union invalidated Privacy Shield and placed additional requirements for companies using standard contractual clauses for data transfers to third countries outside the EU." [43]

The Schrems cases were a fallout of the Snowden revelations, particularly the alleged involvement of Facebook USA in the PRISM or Upstream mass surveillance program under U.S. Foreign Intelligence Surveillance Act (FISA) 702 and Executive Order (EO) 12.333. Schrems campaigned against the violation of privacy rights and EU privacy laws through unauthorized transfers of personal data between the EU and US without "adequate protection" as required under the GDPR. The crux of the Schrems cases was that US laws do not offer sufficient protections against government surveillance of EU citizens' data. Schrems himself had once said in an interview, after the Schrems I decision, that he had nothing personal against the US social network, being an avid user of Twitter and Facebook himself, but his desire was to make communications online safer for people.[44]

---

[42] ibid.
[43] Max Schrems, (*IAPP,* 2023) < https://iapp.org/resources/article/max-schrems/> accessed 21 July 2023.
[44] Julia Fioretti, Shadia Nasralla, and Francois Murphy, "Max Schrems: the Law Student who took on Facebook" (*Reuters*, 7 October 2015) <https://www.reuters.com/article/idUSKCN0S1240/> accessed 23 July 2023.

The journey to the said invalidation of EU-US safe harbor and privacy shield was a circuitous route. It involved complaints filed with the Data Protection Authorities in Ireland, Hamburg, and Belgium, reference(s) to the CJEU, as well as a class action filed in Vienna, Austria comprising over 25,000 Facebook users via the fbclaim.com webpage.

The 16 July 2020 CJEU judgment[45] invalidating the EU-US Privacy shield had resulted in another round of negotiations and adequacy decision on a new framework which was approved in July 2023 as noted earlier above. Reactions seem to suggest it is not yet uhuru for the EU and US on the matter.

It was reported[46] that although European Commissioner for Justice Didier Reynders has said in a press conference that the framework is "substantially different than the EU-U.S. Privacy Shield" privacy advocacy organisation NOYB[47] has criticized the new *EU-US Privacy Framework* as essentially a copy of the old, Privacy Shield (which is in turn a copy of the "Safe Harbor" from 2000) and have indicated that same will be challenged in court. NOYB states that just like "Privacy Shield" the latest deal is not based on material changes, but by political interests. It fails to address "fundamental" surveillance issues.

> *The third attempt of the European Commission to get a stable agreement on EU-US data transfers will be likely back at the Court of Justice (CJEU) in a matter of months. The allegedly "new" Trans-Atlantic Data Privacy Framework is largely a copy of the failed "Privacy Shield."*[48]

NOYB identifies the following areas of concern with the EU-US Privacy Framework:

- The definition of the word "proportionate," The CJEU found that FISA 702 bulk surveillance being not "proportionate" within the meaning of Article 52 of the EU's Charter of Fundamental Rights (CFR).
- The redress via the Privacy Shield "Ombudsperson" – The Data Protection Review Court may not be wholly independent or impartial.
- The US has refused to reform FISA 702 to give non-US persons reasonable privacy protections.
- FISA 702 will have to be prolonged by the end of 2023, given that there is a "sunset clause" in US law.[49]

---

[45] Schrems II Judgment (16 July 2020) in case C-311/18 <https://noyb.eu/files/CJEU/judgment.pdf> accessed 21 July 2023.
[46] Jennifer Bryant, ibid [n 40].
[47] None of Your Business (stylized as *noyb*). NOYB – European Center for Digital Rights is a Non-profit organisation, registered in Vienna, set up in June 12, 2017, for the purpose of promoting data privacy rights, education, and consumer protection globally with a focus in EEA.
[48] Max Schrems, "European Commission gives EU-US data transfers third round at CJEU" (*NYOB*, 10 July 2023) < https://noyb.eu/en/european-commission-gives-eu-us-data-transfers-third-round-cjeu> accessed 12 July 2023.
[49] ibid.

NOYB adds that the motive for going to court is to bring a change to US surveillance laws, to protect the personal data of non-US citizens, engender clear limitations, safeguards, and oversight mechanisms, prevent indiscriminate mass surveillance, and bring clarity to the "Trans-Atlantic Data Privacy Framework" within about two years.[50]

Aside from threats of litigation from NOYB reports surfaced 8 September 2023 that French MP Philippe Latombe filed an application to annul the EU-U.S. Data Privacy Framework.[51]This has the potential of initiating another round of legal limbo for companies in respect of international data transfers between the EU and US. The Schrems cases already took the lead in shaping EU and global jurisprudence on the subject matter. The direction of political and business compliance remains to be seen.

Broadly speaking there are two main routes by which an adequacy decision (as with other EU regulatory instruments) can be struck down.

- A ruling by the EU General Court, having adjudicated on a direct action for annulment [under Article 263 of the Treaty on the Functioning of the European Union (TFEU)[52]].
- A ruling by the Court of Justice of the EU, having received a request for preliminary reference on a point of EU law from a member state court (under Article 267 of the TFEU).

Are we off to another round of litigations, uncertainty and negotiations related to EU-US data transfers? Only time will tell as the data privacy professionals' community monitors developments in the EEA.

3.0 Enforcement Actions Under GDPR

Besides the Schrems I and II, Data Protection Authorities (DPAs) in the EEA through enforcement actions and sanction continue to demonstrate the repercussions companies will face if they fail to meet the core principles of the EU General Data Protection Regulation. As noted above there is a two-tier regime of penalties for high level and low-level offense ranging from the greater of a maximum fine of €20 million or 4% of global annual revenue for the high-level infringements and a maximum fine of €10 million or 2 % global annual revenue (whichever is higher) for low categories respectively. In five years of being in effect, the GDPR has witnessed big fines and

[50] ibid. Schrems predicts that a challenge would reach the CJEU by the end of 2023 or beginning of 2024. The CJEU would then have the option to suspend the "Framework" for the time of the proceedings. A final decision by the CJEU would be likely by 2024 or 2025.
[51] Laura Kayali, "French lawmaker challenges transatlantic data deal before EU court" (Politico, 7 September 2023) < https://www.politico.eu/article/french-lawmaker-challenges-transatlantic-data-deal-before-eu-court/> accessed 8 September 2023.
[52] EUR-Lex, <https://eur-lex.europa.eu/EN/legal-content/summary/annulment-of-legal-acts-by-the-court-of-justice.html.> accessed 20 September 2023.

penalties through enforcement actions by DPAs against big social media and e-commerce companies[53] and violators of GDPR principles for data processing and international data transfers.[54]

3.1 Meta's Instagram and OpenAI

In September 2022 the Irish DPC fined Meta's Instagram 405 million euros over alleged issues with user settings for children 13-17 years old.[55] Then the Italian DPA, *Garante,* temporarily banned ChatGPT, an advanced chatbot developed by OpenAI due to privacy concerns in April 2023.[56] AI usage, Generative AI in particular has initiated privacy rights concerns amongst DPAs and users/data subjects in the EU.[57]

3.2 Facebook

In May 2023 the EU imposed a €1.2bn (£1bn) fine on Meta (owners of Facebook) and ordered the company to stop transferring/sharing the personal data of its European users to the US.[58] Meta's infringement was grave as it involved massive transfers of the personal data of millions of Facebook users in Europe, that have been described as "systematic, repetitive, and continuous." The fine, which is the highest to date under the five-year-old EU General Data Protection Regulation, was accompanied by an order requiring Meta Ireland-owned Facebook to suspend future transfers of personal data to the U.S. within five months of the DPC's decision and to bring its processing operations into compliance "by ceasing the unlawful processing, including storage, in the U.S. of personal data" of EU and European Economic Area users within six months of the DPC's notification to Meta.[59]

---

[53] Thejus Zachariah, "Five Years of GDPR: A Look Back at the Impact of the EU's Data Protection Law" (*Webtoffee*, 8 September 2023) < https://www.webtoffee.com/gdpr-five-years/#:~:text=the%20big%20question%3A-,What%20to%20Expect%20in%20the%20Future%3F,to%20introduce%20their%20privacy%20laws> accessed 3 October 2023. [Facebook's 1.2 billion and Amazon's 746 million euros fines are the biggest to date.]

[54] GDPR Enforcement Tracker (*CMS,* 2023) < https://www.enforcementtracker.com/> accessed 3 October 2023.

[55] "Irish DPC issues 405 M Euro Children privacy fine against Instagram," (*IAPP,* 6 September 2022) <https://iapp.org/news/a/irish-dpc-issues-405m-childrens-privacy-fine-against-instagram/>. See also Vincent Manancourt, "Instagram fined €405 M for violating kids' privacy," (*Politico*, 5 September 2023) < https://www.politico.eu/article/instagram-fined-e405m-for-violating-kids-privacy/> accessed 18 September 2023.

[56] Shiona McCallum, "ChatGPT banned in Italy Over Privacy Concerns" (*BBC News,* 1 April 2023) <https://www.bbc.com/news/technology-65139406> accessed 19 September 2023.

[57] Ibid.

[58] Chloe Kim, "Privacy activists slam EU-US pact on data sharing" (*BBC News*, 11 July 2023) <https://www.bbc.com/news/world-us-canada-66161135> accessed in 19 Sept 2023. See also Jedidiah Bracy, "Meta fined GDPR-record 1.2 billion Euros in data transfer case" (*IAPP,* 22 May 2023) < https://iapp.org/news/a/meta-fined-gdpr-record-1-2-billion-euros-in-data-transfer-case/ > accessed 20 September 2023.

[59] Jedidiah Bracy, ibid.

3.3 OpenAI's ChatGPT

In August 2023 a privacy and security researcher with a law firm based in Warsaw, *Lukasz Olejnik*, had also filed a complaint, with the Poland's Office for Personal Data Protection (DPA),[60] against OpenAI's, ChatGPT, for multiple violation of GDPR[61] in the areas of unlawful processing of training data, fairness, transparency, data access rights, and privacy by design.[62]

3.4 TikTok

More recently, Ireland's DPC fined Tik Tok 345 Million for violation of the core principles of GDPR concerning children's data protection in September 2023.[63] The enforcement action concerned claims against TikTok's platform settings for kids that it had in place over a five-month span 31 July 2020 to 31 December 2020. The DPC investigation yielded violations of Articles 5(1)(c), 5(1)(f), 12(1), 13(1)(e), 24(1), 25(1) and 25(2) while an additional violation of Article 5(1)(a) was added following the European Data Protection Board's August binding decision on the matter.[64]

TikTok's penalty closely aligns with the 405 million euro fine issued to Meta's Instagram in September 2022 over alleged issues with user settings for children 13-17. Both instances scrutinized the companies' respective use of a "public-by-default setting" with children's accounts.[65]

TikTok, Snapchat and Instagram are quite popular among young content creators and social media users. Facebook is more popular with older (working class/middle-aged) and elderly[66] users.

4.0 The Future of Data Privacy and Protection

The EU through the GDPR has indeed recorded a number of successes in the last five years of its existence and it is hoped that it would continue to do so in the future. GDPR has set the foundation for a new era of data protection and privacy, emphasizing transparency, compliance, and the

---

[60] *Urząd Ochrony Danych Osobowych*.
[61] arts 5, 12, 15(1)(a) and (c),16, 25(1) and 36 GDPR.
[62] Scott Ikeda, "OpenAI Complaint Filed with Polish DPA Alleges Multiple GDPR Violations" *CPO Magazine* (5 September 2023) < https://www.cpomagazine.com/data-protection/openai-complaint-filed-with-polish-dpa-alleges-multiple-gdpr-violations/> accessed 19 September 2023. See also Natasha Lomas, "ChatGPT-maker OpenAI accused of string of data protection breaches in GDPR complaint filed by privacy researcher" (*Tech Crunch,* 30 August 2023) < https://techcrunch.com/2023/08/30/chatgpt-maker-openai-accused-of-string-of-data-protection-breaches-in-gdpr-complaint-filed-by-privacy-researcher/ > accessed 31 August 2023.
[63] Joseph Duball, "Ireland's DPC Issues 345M Euro TikTok Children's Privacy Fine" (*IAPP*, 15 September 2023) <https://iapp.org/news/a/irelands-dpc-issues-345m-euro-tiktok-childrens-privacy-fine/> accessed 19 September 2023.
[64] ibid.
[65] ibid.
[66] My mum, aunties and uncles are septuagenarians, and they are avid users of Facebook. It might be safe to conclude Facebook is definitely a Gen X and Baby Boomer app.

integration of privacy measures into all operations.[67] This author predicts that we would see more collaborations with countries and companies in the area of adequacy decisions, the use of BCRs and SCCs for international transfers; More data privacy impact and risks assessments and the adoption of Privacy by design and default as well as Privacy Enhancing Technologies in respect of new technologies; Data Localisation; Web 3.0; and AI Governance through the EU AI Act.

4.1 Adequacy Decisions: EU, US, and the California Effect

Articles 44-46 of the GDPR relate to adequacy decisions in respect of international data transfers. The idea is that a recipient country should provide data protection essentially equivalent to the protection provided in the EU. It is expected that, with the recent EU-US Data Privacy Framework and the UK-US Data Bridge, more adequacy decisions and data transfer arrangements would be reached between the EU and other countries.[68] I dare say even with sub-nationals like the state of California given its av*ant-garde* California Privacy Rights Act (CPRA) which is setting the standards[69] for US State data protection laws.[70]

Several of the new CPRA provisions are based on GDPR principles and have been suggested to perhaps be with an eye towards obtaining an adequacy decision from the European Commission. While balancing transparency, choice, and flexibility for technological development, the CPRA also contains unique elements that set it apart from any privacy statute in the world.[71] The CPRA's enhanced privacy protections seem clearly meant to place California as an adequate jurisdiction to which companies in European Union (EU) Member States can transfer data pursuant to Article 45 GDPR. Thus, a decision by the European Commission that California provides an adequate level of data protection for cross-border transfers from the EU would be welcomed and unprecedented for any state in the US. Such a decision could encourage other states to adopt privacy legislation similar to the CPRA. However, whether the European Commission would be prepared to take such a bold step is unclear, particularly because the EU Court of Justice raised concerns in Schrems II regarding the scope of certain US federal laws (Section 702 of the Foreign Intelligence Surveillance Act, Executive Order 12333, and Presidential Policy Directive 28). Since those laws apply to companies in California, the European Commission might find it difficult to grant the state adequacy and still comply with the reasoning in Schrems II.[72] Nevertheless this is an interesting point to note and ponder, while we await the unravelling of time.

---

[67] Privacy Engine, "GDPR 5th Anniversary: Everything You Need to Know" (*Privacy Engine*, 24 May 2023) <https://www.privacyengine.io/blog/gdpr-5th-anniversary/> accessed 3 October 2023.

[68] cf. OECD and Global CBPR Forum. See Joe Jones "UK-US Data Bridge Becomes Law, Take Effect 12 Oct." (*IAPP,* 21 September 2023) < https://iapp.org/news/a/uk-u-s-data-bridge-becomes-law-takes-effect-12-october/> accessed 2 October 2023.

[69] California Effect.

[70] Michelle A Reed and others, "CPRA Rivals GDPR's Privacy Protections While Emphasizing Consumer Choice." (*Akin,* 11 November 2020) < https://www.akingump.com/en/insights/alerts/cpra-rivals-gdprs-privacy-protections-while-emphasizing-consumer-choice#:~:text=Several%20of%20the%20new%20CPRA%20provisions%20are%20based,obtaining%20an%20adequacy%20decision%20from%20the%20European%20Commission.> accessed 3 October 2023.

[71] Right to Correct, Data Minimization, Purpose Limitation and Data Retention, Risk Assessment, Automated Decision Making, Independent Regulatory Agency, Two tiers of Consumer Data (Personal Information and Sensitive Personal Information), Protection of Onward Data Transfers; Incentives for Enhanced services; and Opt-out Preference Signals.

[72] Michelle A Reed and others, ibid.

4.2 DPIA, PbD, PETs and RoPA

Privacy by Design (PbD), Privacy Enhancing Technologies (PETs), Records of Processing Activities (RoPA) and Data Protection Impact Assessment (DPIA) are measures that may be taken to ensure GDPR compliance and to regulate new technologies and activities that may be considered high risk to the freedoms and rights of data subjects.

Article 25 GDPR requires privacy by design to be integrated by companies in processes and new technologies being developed. The European Data Protection Supervisor Giovanni Buttarelli set out the requirement to implement privacy by design in an article.[73] The concept of PbD was developed by Information and Privacy Commissioner of Ontario, Canada, Ann Cavoukian in 1995. A privacy by design workshop was co-hosted by her in 2009.[74] In 2010 the framework achieved international acceptance when the International Assembly of Privacy Commissioners and Data Protection Authorities unanimously passed a resolution on privacy by design.[75]

PbD is a technique that incorporates strong privacy practices into the design and implementation of technology systems.[76] The foundational principles outlined by Cavoukian entail privacy as a default setting; privacy embedded into design; with end-to-end security; full functionality; full lifecycle protection; transparency and respect for user privacy. PbD ensures that personal data are automatically protected in any IT system or business practice. PETs on the other hand involve technologies that embody fundamental data protection principles by data minimization, use and purpose limitation, maintaining confidentiality, maximizing data security, and empowering individuals. PETs may be used for data de-identification and anonymisation, by removing those elements used to identify the individual in order to make the information non-personal.[77]

Article 30 GDPR requires data controllers and processors to keep a record of processing activities (RoPA). This record is intended to ensure GDPR compliance and extend consumer data protection to businesses that handle Big Data (including internet businesses). The RoPA contains information about purpose of processing, lawful basis, category of personal data processed, recipients of personal data, information on transfers, security measures et al and the record must be provided to the Data Protection Authority (DPA) on request.[78] Article 35 of the GDPR requires data controllers and processors to conduct a data protection impact assessment (DPIA) before using new technologies to process personal data where such activity is likely to result in **high risk to the**

---

[73] G Buttarelli, "Privacy by Design: Privacy Engineering" Jan 25, 2018, EU. <18-01-25_privacy_by_design_privacy_engineering_cpdp_en_3.pdf (europa.eu)> accessed 7 September 2023.

[74] Ann Cavoukian, "Privacy by Design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D." *Identity in the Information Society*. (2010) 3 (2): 247–251. <doi:10.1007/s12394-010-0062-y. S2CID 144133793.> accessed 9 September 2023.

[75] "Video Rewind: 'Privacy by Design' approach gains international recognition" (*ITbusiness.ca,* 4 November 2010) <https://www.itbusiness.ca/news/video-rewind-privacy-by-design-approach-gains-international-recognition/15626> accessed 10 September 2023.

[76] For instance, to enhance user privacy the new Microsoft 365 Copilot neither retains user's prompts nor use them to train its Large Language Model (LLM). See "How Microsoft 365 Copilot Works" (*YouTube*, September 2023) <https://www.youtube.com/watch?v=B2-8wrF9Okc&t=440s > accessed 4 October 2023.

[77] Other examples of PETs include - *Obfuscation, Communication Anonymisers, Blinding, Ring Signature, Enhanced privacy ID, Format-preserving encryption, Homomorphic encryption, Adversarial stylometry, Zero-knowledge proof.*

[78] art 30(1) – (5) GDPR

rights and freedoms of natural persons.[79] A DPIA[80] is a mandatory process designed, in specific instances prescribed by the GDPR, to aid organisation's systematically analyse, identify and minimise the data protection risks of a project or plan. DPIAs are required when a high-risk process is being initiated or such existing process is being modified and it is done in collaboration between the business and data protection team with a view to identifying and assessing privacy risks and to determine appropriate measures to mitigate those risks. Examples of instances requiring a data protection impact assessment include automated decision-making (like using AI Systems), profiling, large scale processing of special categories of data, records of criminal conviction, and systematic monitoring of a publicly assessable area on a large scale.[81]

The DPA is expected to provide a blacklist and whitelist of processing operations that require or do not require DPIAs.[82] Many DPA's in the EU Region have published draft blacklists od data processing activities that would trigger DPIAs and the EDPB has released an opinion on same.[83] The DPIA shall contain a **systematic description** of the processing operation, **necessity and proportionality** in relation to use purpose, **risks to freedoms and rights** of the data subject; and **security measures** for addressing such risks.[84]

4.3 Data Localisation

Data localisation or data residency law requires personal data to be collected, processed, and/or stored inside the country of origin, prior to being transferred internationally. Such data may only be transferred after satisfying the requirements of local data privacy and protection laws, such as notice about the use of the data and obtaining consent of the data subject before processing.
In 2005 Kazakhstan moved towards data localization by requiring that all ".kz" domains to be run locally (with later exemption for Google).[85] The Edward Snowden revelations regarding United States counter-terrorism surveillance programs in 2013, however, ignited a worldwide[86] push for data localisation worldwide.[87]

---

[79] art 35(1) GDPR
[80] cf. PIA (Privacy Impact Assessment) which is similar but not a requirement of GDPR as is the case with DPIAs. It is a pre-GDPR term. PIAs are generally performed for the benefit of the project or organization itself rather than strictly for the protection of personal data or data subjects. Privacy impact assessments are conducted for the establishment of new or improved projects, developments, or undertakings that might result in privacy risks. They are also conducted when processes involving personal information are changed. Conducting a PIA ensures that privacy is at the forefront of every project or data processing engagement. DPIAs and PIAs differ in respect of focus and benefits. The former focuses on and is for the benefit of the data subject, while the latter focus is on privacy risks and for the benefit of the project and the organisation. A PIA assesses the risks posed throughout the lifecycle of a data processing project.
[81] art 35(3) GDPR. DPIAs can also be said to help implement PbD and GDPR compliance.
[82] art 35(4) and (5) GDPR.
[83] See IAPP Website < https://iapp.org/resources/article/eu-member-state-dpia-whitelists-and-blacklists/ > accessed 4 October 2023.
[84] art 35 (7) GDPR. DPIA has four elements – Systematic description; assessment of necessity and proportionality; risks to data subject's freedoms and rights; and security measures.
[85] Anupam Chandra and Uyen P Le, "Data Nationalism" (2015) 64 Emory LJ 677, 682.
< https://scholarlycommons.law.emory.edu/cgi/viewcontent.cgi?article=1154&context=el> accessed 5 October 2023.
[86] France and Germany took the lead in Europe at the time.
[87] A Chandra, ibid 679.

Data localisation is considered in some quarters as protectionist and a barrier to trade. The EU believes that data localisation should be left to the EU to regulate at a pan-EU level, and member states' domestic data localisation laws would violate European Union competition law.[88] The EU made this evident by passing the GDPR. The EU's GDPR contains extensive provisions regulating data flow and storage, including restrictions on exporting personal data outside of the EU.[89]

Australia, Germany, and China are advocates and supporters of data localisation in some form or entirely in respect of medical records, telecom metadata, personal, business, and financial data.[90]

4.4 AI Governance

The proliferation and adoption of Artificial Intelligence (AI) in recent years has stirred interest about the potential of AI as well as genuine concerns about the risks of AI. There are two broad AI, namely Generative AI (GenAI) for generating content, such as text, images, video, and audio (OpenAI's ChatGPT and GPT4 being the most popular alongside DALL E, Midjourney, Stable Diffusion, and more recently Microsoft 365 Copilot) and Predictive AI for analytics and predicting outcomes. Predictive AI and Generative AI are based on machine learning techniques. They rely on algorithms and models that learn patterns and structures from data sets.[91]

Both GenAI and Predictive AI show promise and potential application in the field of medical research, astronomy, business, healthcare diagnostics and treatment, financial investment, stock market predictions, weather forecast, generating content for gaming, marketing campaign, movies, autonomous vehicles and robotics, military, education, audit, fraud detection and law enforcement. AI however has its risks. The dual use risk (for good or bad by terrorists or criminal elements[92]), creator bias and algorithm bias. At the point where the potential and risks of AI converge is where AI Governance finds relevance and impetus for implementation.

U.S. Executive Order 13960 requires federal agencies to specify responsible officials and provide appropriate training for AI governance. The proposed Canadian code of practice for generative AI systems envisages the designation of responsible staff, while drafts of the EU AI Act would require human oversight of high-risk AI systems with the necessary competence, training, and authority.[93]

---

[88] Which frowns upon anti-competitive conduct and monopolies by companies that affect public interest.

[89] Without an adequacy decision, use of SCCs or BCRs, or under derogations (arts 45, 47, 49 and 93 GDPR).

[90] Other counties include – Canada (in the provinces [of Nova Scotia and British Columbia] – all personal data), India (payment system data), Indonesia (public service companies data), Kazakhstan (servers running on country domain), Russian (all personal data), Rwanda (all personal data), Nigeria (all govt data), South Korea (geospatial and map data), Spain (election roll, fiscal data, census and health records must be processed within the EU), Vietnam (service providers usage data).

[91] "Generative AI Vs Predictive AI: Unveiling the Differences" (*Rezo.AI*, 8 September 2023) < https://rezo.ai/our-blogs/generative-ai-vs-predictive ai/#: ~:text=Generative%20AI%20and%20 Predictive%20AI %20are%20two% 20subfields, of%20processes%20using%20complex%20mathematical%20calculations%20on%20data.> accessed 5 October 2023.

[92] There are reports of dark AI or malicious AI on sale on the dark web – *WormGPT, FraudGPT, PoisonGPT, WolfGPT,* and *XXXGPT.* See Tim Keary "The Future of Dark AI Tools: What to Expect Next?" (*Techopedia,* 1 September 2023) < https://www.techopedia.com/the-future-of-dark-ai-tools-what-to-expect-next > accessed 5 September 2023.

[93] J Trevor Hughes, "The Time to Professionalize AI Governance is Now" (*IAPP,* 2 October 2023) < https://iapp.org/news/a/the-time-to-professionalize-ai-governance-is-now/> accessed 10 October 2023.

The EU is in the process of enacting an AI Act to provide clarity on AI Governance.[94] The EU AI Act went into the process of trilogue negotiations in August 2023.[95] In Canada the AI and Data Act,[96] part of the Omnibus Bill C-27 is poised to change the regulation of the Data and AI systems.[97] These developments are positive ones and in the interim the GDPR,[98] the OECD AI Principles,[99] and the NIST AI Risk Management Framework (AI RMF 1.0)[100] would continue to be applied to dictate data privacy standards and principles relating to ethical and responsible deployments of AI.

4.5 Web 3.0 and Data Privacy

The term "Web3" was coined in 2014 by Ethereum co-founder Gavin Wood, and the idea gained interest in 2021 from cryptocurrency enthusiasts, large technology companies, and venture capital firms.[101] Web 3.0 is the next generation of decentralized internet, providing a more personalized and interactive experience while giving users more control over their personal data and privacy.[102]

The journey to Web 3.0 has witnessed two prior iterations. Web 3.0 being described as the third iteration of the world wide web. Web 1.0[103] (1994 - 2004) comprised all read only content, which was static and not interactable. It was similar to a huge Wikipedia page. Web 2.0 (2004 - date) Focused on interactivity, interoperability, and collaboration. It has been described as a “read-write web.” Developments in web technology such as HTML 5, Java Script and CSS3 made it possible for the creation of such interactive platforms as Facebook, YouTube, Wikipedia and many more. With the introduction of blogs, wikis and social media sites, web users were no longer just passive content consumers; they could now create content and share it online.[104]

---

[94] ibid

[95] Muge Fazlioglu “Contentious Areas in the EU AI Act Trilogues” (*IAPP,* 30 August 2023) < https://iapp.org/news/a/contentious-areas-in-the-eu-ai-act-trilogues/> accessed 3 September 2023

[96] Artificial Intelligence and Data Act (AIDA) companion document (Government of Canada, 2023) < https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document> accessed 11 October 2023.

[97] Caitlin Fennessy “Regulators’ Rulebook for AI: Bit by Bit” (*IAPP*, 2 August 2023) < https://iapp.org/news/a/regulators-rulebook-for-ai-bit-by-bit/.> accessed 11 October 2023.

[98] arts 5, 9, 25 and 30 GDPR.

[99] OECD < https://www.oecd.org/digital/artificial-intelligence/> accessed 1 October 2023

[100] NIST (January 2023) < https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf> accessed 29 September 2023.

[101] Gilad Edelmann, “The Father of Web3 Wants You to Trust Less” (*Wired,* 29 November 2021) < https://www.wired.com/story/web3-gavin-wood-interview/> accessed 7 October 2023.

[102] Shubham Gupta, “What Is Web 3.0, and How Does It Impact Digital Marketers?” (*Gartner Digital Markets*, 27 May 2022) <https://www.gartner.com/en/digital-markets/insights/what-is-web-3-0#:~:text=Increased%20privacy%20and%20security%20are%20the%20chief%20features,data%20and%20what%20they%20can%20do%20with%20it.> accessed 11 October 2023.

[103] The first generation, referred to as Web 1.0, was invented in 1989 by Tim Berners-Lee, a British computer scientist who applied the hypertext concepts for linking digital text proposed in 1963 by Ted Nelson, an American information technology pioneer. Besides programming the first browser, Berners-Lee wrote the Hypertext Markup Language (HTML), which tells browsers how to display content, as well as the Hypertext Transfer Protocol (HTTP) specifying how web servers transfer files to browsers. He also started designing software for a "Semantic Web" that would link data across web pages, but hardware constraints prevented its implementation. See David Essex, Sean Michael Kerner, and Alexander Gillis, “What is Web 3.0 (Web3)? Definition, guide, and history” (*TechTarget,* September 2023) <https://www.techtarget.com/whatis/definition/Web-30> accessed 7 October 2023

[104] Shubham Gupta, ibid. See also Simplilearn, “We 3.0 Explained in 5 Minutes” (*YouTube*, 17 May 2022) < https://www.youtube.com/watch?v=0tZFQs7qBfQ> accessed 11 October 2023.

Web 3.0 is a "read-write-execute web" or "read-write-interact web." It focuses on interaction and collaboration between humans and machines. It is also known as semantic web[105] and is an extension of the World Wide Web that uses standards set by the World Wide Web Consortium (W3C). It aims to make the Internet smarter by handling information with human-like intelligence using artificial intelligence systems.[106] The web is becoming increasingly intelligent and adaptable with the advent of new technologies, including semantic web, ai, cryptoassets & blockchain, natural language processing and machine learning. It is said to decentralize control and monopoly over big data by big tech companies like Google, Meta and Amazon as is the case with Web 2.0. When a user carries out a search online or browses the internet, information about the user's activities, IPs, preferences, search, and browsing history are stored in cookies which are used to build a definitive online user profile of the individual which may later be sold to other companies for behavioral marketing and ad targeting purposes without the knowledge or consent of the individual. Web 3.0, is largely still being developed but when fully implemented as envisioned, a decentralized, semantically aware version of the web via ai and natural language processing, will fundamentally change how big tech companies collect, centralize, and monetize petabytes of customer data.[107]

It is important at this juncture to point out that although both web3 and web 3.0 are similar, in names and have a common purpose, there is a huge difference in their concepts and approach. Both web3 and web 3.0 aim to create a better version of the Internet by maintaining users' control over their data. The core difference, however, lies in the storage of data in a solid pod in the semantic web, while web3 uses decentralized technologies for the same.[108] Many consider web3 the same as 3.0. They believe the future of the web will be an integration of vital web 3.0 elements like machine-readability, and web3 aspects like blockchain or the metaverse.[109]

Web 3.0 would be comprised of a global peer-to-peer (P2P) network with no third-party intermediary or need for approval thus it shall be trusting and permissionless, have more control over web content, greater transparency, and accountability with a decentralized immutable blockchain ledger, which will better balance privacy protection and personalisation. The Key features of Web3 or Web 3.0 include – **decentralised** structure based on a distributed and

[105] Tim Berners-Lee coined the term "Semantic Web," which refers to a version of the web that can connect everything at the data level. The goal of the semantic web is to make internet data machine readable. The publishing language (e.g., RDF, OWL, and XML) is designed to enable the encoding of semantics with the data, thus the machine-readable descriptions enable content managers to add meaning to the content, i.e., to describe the structure of the knowledge we have about that content. In this way, a machine can process knowledge itself, instead of text, using processes similar to human deductive reasoning and inference, thereby obtaining more meaningful results, and helping computers to perform automated information gathering and research. While HTML on the other hand may be limited to such markup fields as keywords or author. cf. metadata tags.

[106] Akash Takyar, "Web3 v. Web 3.0: How Are They Different" (*LeewayHertz*, 2023)
< https://www.leewayhertz.com/web3-vs-web3- 0/#: ~:text=Although%20most%20discussions%20revolving %20around%20the%20third%20generation, Berners-Lee%E2%80%99s%20concept%20of%20a%20linked%20or% 20semantic%20web.> accessed 7 October 2023.

[107] David Essex et al, ibid [103].

[108] Akash Takyar, ibid.

[109] ibid.

democratic approach devoid of a central authority,[110] **blockchain based** immutable distributed ledger in which data is managed and validated on a P2P network which helps to verify authenticity and build trust amongst users, **cryptocurrency enabled** which will replace "fiat currency" issued by government central banks, **user control and privacy** over online identity and personal data independent of central providers and big tech companies, **semantically organized** for better search and content generation, **resilience** as it is decentralized and less vulnerable to single point failure, **transparency** due to blockchain decentralization which promotes better transactions and decisions visibility, **connectivity and ubiquity** so the IoTs will no longer be limited to PCs and smart devices, and **autonomous and artificial intelligence** powered websites with the ability to better understand user intention and preferences and automatically curate and deliver content saving companies time and money.[111]

These attributes of Web 3.0 have been identified as the reason Web 3.0 might just be the solution to data privacy and protection in a booming and rapidly expanding digital economy. Web 3.0 promises open, trustworthy, and permissionless networks. That is not overlooking the complexity, costs, technical requirements and learning curve involved in the transition to Web 3.0 coupled with regulatory concerns and security risks raised from the hacking of smart contracts and cryptoassets exchanges reported on the news. However, the Web 3.0 trend is here to stay and the predicted timeframe[112] for full implementation may be enough to address all the potential risks and challenges.[113]

5.0 Conclusion

The GDPR has been in effect for five years, from May 2018. In that time the GDPR has increased individual awareness about their data privacy rights and more control over the collection and processing of their personal data. It also sparked off international convergence on data privacy standards and seen the passage of the other data protection laws modelled after it by countries in the EU, Africa, Asia, and Latin America.[114] It is expected that other countries (at the national and sub-national levels) would pass similar laws in the near future to engender data privacy and security following the convergence and mass adoption of Big Data, AI, IoT and Smart devices. The EU AI Act like the GDPR is expected to set the standard for AI Governance. More

[110] Decentralized Autonomous Organizations (DAOs) may provide the structure and governance needed in Web 3.0 by wresting control from central authorities and devolving it to self-governed digital communities. DeFi, Smart Contracts, Metaverse, NFTs, and dApps will also form part of Web 3.0 use cases and applications.
[111] David Essex et al, ibid.
[112] Ten to fifteen years judging from the earlier iterations (Web 1.0 and 2.0).
[113] David Essex et al, ibid.
[114]See India, Nigeria, US, and Canada et al; - Securiti Research Team,
"Data Privacy Laws and Regulations Around the World," Published November 8, 2021, Updated August 24, 2023,
< https://securiti.ai/data-privacy-laws > accessed 10 September 2023; and
M Fazlioglu, "US Federal Privacy Legislation Tracker Introduced in the 118th Congress (2023-2024)"
< https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf > accessed 4 October 2023.
cf. Brussel Effect and Delaware Effect.

countries[115]and sub-nationals[116] have data protection laws billed to come into effect in the near future.[117] The domino effect of some of these laws may lead other jurisdictions to update their laws as well.[118]

There were also big fines and penalties recorded against big social media and e-Commerce companies following enforcement actions for noncompliance with the GDPR principles and improper international data transfers. Similarly, there were increased data breach reports to the authorities and victims within the 72 hours timeframe as required by the GDPR. Greater compliance is expected in the future as companies and data privacy professionals transition in the core of their activities and outcomes in privacy risk management from a reactive and advisory role, to a transparent, agile and risk informed approach that fosters accountability.[119]

Asia and Africa are jurisdictions to watch as there is increased activity in the digital space by the public and private sector stakeholders in an attempt to leverage and optimize dividends of the digital economy to shore up dwindling reserves through alternative sources, distinct from agriculture, tourism, oil, and solid minerals.[120]

May we continue to live in interesting times.

---

[115] Securiti Research Team,
"Data Privacy Laws and Regulations Around the World," Published November 8, 2021, Updated August 24, 2023,
< https://securiti.ai/data-privacy-laws > accessed 10 September 2023.

[116] See Quebec Bill 64; and M Fazlioglu, "US Federal Privacy Legislation Tracker Introduced in the 118th Congress (2023-2024)"
< https://iapp.org/media/pdf/resource_center/us_federal_privacy_legislation_tracker.pdf > accessed 4 October 2023.

[117] For example, the Saudi Arabia Personal Data Protection Law (PDPL) passed March 2023 with a compliance grace period till September 2024; Indonesia PDPL passed Sept 2022 allowing organisations 2 years to fully comply.

[118] Quebec Bill 64 and CPRA may have this effect.

[119] NIST Privacy Framework (16 January 2020)
<https://www.nist.gov/system/files/documents/2020/01/16/NIST%20 Privacy%20Framework_V1.0.pdf> accessed 28 July 2023.

[120]In November 2019 the Nigerian Government issued the National Digital Economy Policy and Strategy (2020-2030) to develop the digital economy and facilitate diversification of the economy (*NITDA*, November 2019)
< https://nitda.gov.ng/wp-content/uploads/2020/11/National-Digital-Economy-Policy-and-Strategy2.pdf#:~:text=The%20National%20Digital%20Economy%20Policy%20and%20Strategy%20has,from%20dependence%20on%20the%20oil%20and%20gas%20sector.> accessed 3 September 2023; and in August 2023 the Minister for Communications and Digital Economy called on experts to help co-create a National AI Strategy. See (X, formerly Twitter, 28 August 2023) <https://twitter.com/bosuntijani/status/1696113557354549599> accessed 3 September 2023.