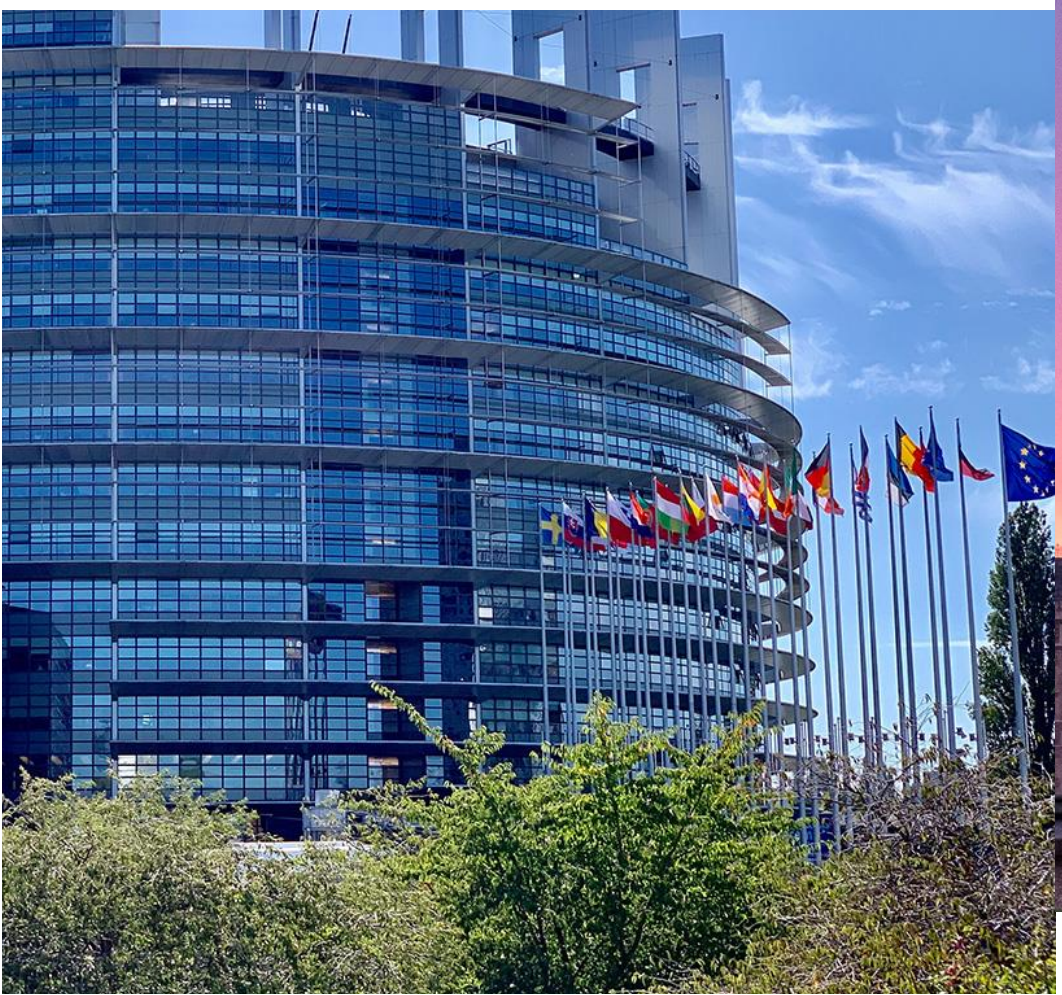
British Institute of International and Comparative Law

Disaggregation of Digital Information and Data Sovereignty Compliance

Iris Anastasiadou | Dr Julinda Beqiraj | Dr Jean-Pierre Gauci

February 2023



British Institute of International and Comparative Law

The British Institute of International and Comparative Law (BIICL)

BIICL is one of the leading independent research centres for international and comparative law in the world. Our high quality research projects, seminars and publications encompass almost all areas of public and private international law, comparative law and European law, and we are at the forefront of discussions on the many contemporary issues of international and comparative law. BIICL includes within it the innovative Bingham Centre for the Rule of Law, which has a particular focus on the many rule of law issues world-wide.

* Iris Anastasiadou is Researcher in Public International Law and Migration at BIICL.

* Dr Julinda Beqiraj, is the Maurice Wohl Senior Fellow in European Law at the Bingham Centre for the Rule of Law (at BIICL).

* Dr Jean-Pierre Gauci is the Arthur Watts Senior Research Fellow in Public International Law and Director of Teaching and Training at BIICL.

Table of Contents

Executive Summary

Trends show that most of the computing activity that is performed locally on end-user computers will eventually shift into the Cloud. Yet, reliance on cloud resources that are controlled by third parties, and whose use is shared, comes with risks, mainly related to reduced/loss of customer control and increased service provider control of data in clouds, risks over data security, and lack of transparency regarding the locations of providers. The huge amount of data stored outside of national boundaries has become a critical issue that is closely related to the question of government control over domestic data (i.e., data sovereignty), where rules introduced by states may result in both protection and limitations for companies that wish to resort to cloud services.

The paper aims to assess the legitimacy of Prizsm Technologies' assertion that data sovereignty rules are upheld if digital information is disaggregated and disbursed across multiple geographic jurisdictions through the Prizsm Platform. Our assessment, made in the light of desk-based research of existing academic and grey literature, and comparative legal analysis of the legislation from selected national jurisdictions, highlights the following findings.

- Data protection laws in the various jurisdictions assessed introduce restrictions in relation to the processing, storage, management and transfer (including import and export) of identified or identifiable personal data. Such restrictions do not apply when data is anonymised and does not allow identification.
- Our understanding of the Prizsm Platform is that it would allow users to comply with the regulations on data protection that operate where the storage provider is located, because restrictions only apply to identifiable personal data. Prizsm, moreover goes beyond anonymisation of data (both personal and other data), and disaggregates data at the bit level, making it nearly-impossible to retrieve the original information without the 'Prizsm key'.
- The random allocation of the disrupted binary digits across multiple cloud endpoints (through Prizsm) would increase protection against security breaches and would help prevent and/or avoid risks related to unauthorized access to cloud data (by the storage provider, hackers, or governments), because in such an event all that can be accessed is a random fraction of binary digits, unintelligible on its own.
- The Prizsm approach relying on diversification of storage services seems a secure and resilient one that reduces security risks – any damage, loss, or unwarranted access of data stored with a specific storage provider would only affect a random set of binary digits – while also ensuring continued availability of data in the event of loss of functionality, end of business of the storage platform or data corruption. Based on our understanding of the way Prizsm operates, the algorithm would be able to recalculate the missing digits stored in the corrupted cloud endpoint, and thereby allow the user to gain access to the original information, provided that the key is available which is something only data owners would have.
- On the contrary, any attempt to hack or otherwise access data (including by law enforcement under powers granted through legislation) would only reach a series of

disrupted binary digits which on their own are unintelligible. The storage provider would not be in a technical position to access or provide to the authorities intelligible data because no such intelligible data will be stored with any one storage provider.

- Despite the safe solution for multi-cloud digital information storage offered by Prizsm, Prizsm platform users, as the main controllers of the Platform and its keys must invest in security measures at their end.

1. Introduction

There is a trend showing that most of the computing activity that is performed locally on end-user computers will eventually shift into the Cloud. Yet, reliance on cloud resources that are controlled by third parties, and whose use is shared, comes with risks. Concerns are mainly related to reduced/loss of customer control and increased service provider control of data in clouds, risks over data security, and the lack of transparency regarding details and locations of providers, components and suppliers of the service.[1] A specific concern is related to the possibility that data stored on a third party's infrastructure, may no longer be available to the customer/owner if the equipment of the cloud provider is seized, made inaccessible, or if business is closed down.[2] However, customers do not necessarily lose all control on data stored in cloud resources, and measures can be taken to prevent and minimise some of the risks, e.g. through the use of protection gateways at the source that would allow secure storage of the data with one or different cloud providers.

A key concept in this regard is that of 'data sovereignty' which loosely means that governments have control over data 'located' within their jurisdiction (domestic data). Therefore, information stored in the cloud can be subject to a variety of national laws (potentially espousing divergent standards), depending on where data is stored, processed or transmitted.

Data storage, management and processing is increasingly being regulated by states. On the one hand, relevant rules may impose limits requiring providers in third countries to comply with the same standards as those in force in the jurisdiction of the customer, if domestic data is somehow involved, or to limit the circulation of data in countries that would not satisfy those standards (e.g., EU). On the other hand, data sovereignty would allow national authorities to seize, under certain circumstances and under the rules applicable in that jurisdiction, the provider's equipment which may contain data of customers based in other jurisdictions.

This paper aims to assess the legitimacy of Prizsm Technologies' assertion that data sovereignty rules are upheld if digital information is disaggregated and disbursed across multiple geographic jurisdictions through the Prizsm Platform. According to Prizsm Technologies, the "Prizsm Platform provides a secure, easy-to-use, resilient solution for multi-cloud digital information storage". Prizsm is a zero-storage "platform operating through an algorithm that disrupts data at bit-level and pseudo-randomly distributes complementary binary digits to locations across multiple cloud platform endpoints, storing the information securely".

---

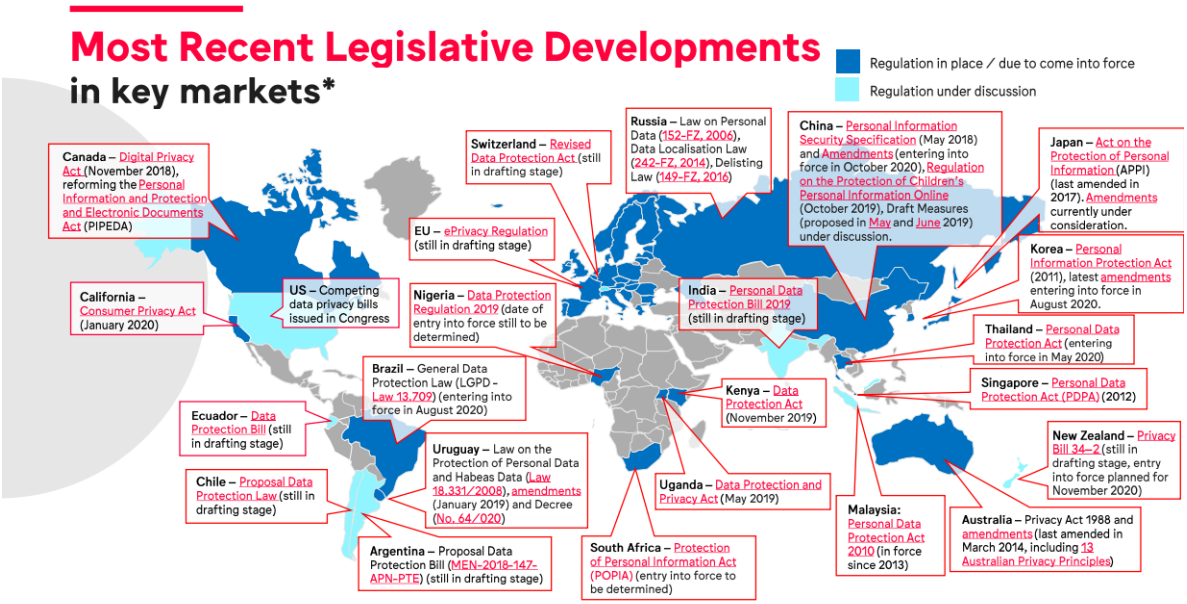
[1] W Kuan Hon, Christopher Millard, and Jatinder Singh "Control, Security, and Risk in the Cloud" Chapter 2, in C. Millard (ed.) Cloud Computing Law, (2nd edn, OUP 2021), https://global.oup.com/academic/product/cloud-computing-law-9780198716679?lang=en&cc=uk#

[2] For instance, risks related to seizure for security purposes (here) or for breaches of the law (here).

The paper assesses such claims in the light of desk-based research of existing academic and grey literature, and comparative legal analysis of the legislation from selected national jurisdictions. The analysis provided here is not and should not be presented as or taken to be legal advice but rather a research based legal analysis based on information available to the researchers. Specific legal advice should be sought before any decisions are made.

2. Analysis

The huge amount of data stored outside of national boundaries has become a critical issue that is closely related to the question of government control over domestic data (i.e., data sovereignty). While companies and governmental agencies may be reluctant to release their data into the Cloud – concerned about the data entering territories where it would become subject to laws allowing for the foreign government to access that data (the US example, see below) – some jurisdictions have tried to address this issue by enacting regulations whereby data cannot be transferred to third countries that do not provide an "adequate level of protection" (the EU example, see below). Accordingly, data sovereignty rules may result in both protection and limitations for companies that wish to resort to cloud services. This area is increasingly being regulated by states (see table below), but legal uncertainties remain that still need to be addressed, preferably through international common standards.



Source: The WFA Global Privacy Map

In the meantime, new initiatives have been made available, that aim to increase awareness regarding the different aspects of cloud security and the respective responsibilities of customers and providers, and to improve cloud security generally.[3] Risks associated with unauthorized access can be prevented or minimized by customers by hiding 'plaintext visibility' of their data before uploading datasets to the cloud. One example is cryptographic applications which may transform datasets, or parts thereof, by applying an 'algorithm' which

[3] Niamh Gleeson and Ian Walden, "Cloud Computing, Standards, and the Law", in C. Millard (ed.) Cloud Computing Law, (2nd edn, OUP 2021). See also Cloud Security Alliance, 'Cloud Controls Matrix' https://cloudsecurityalliance.org/research/ccm .

would translate information into another 'language' so that only those knowing that 'language' can understand the translation. Other ways to protect data have been developed, and more are likely to emerge, including tokenisation systems – widely used in relation to payment card data – which are mapped to and reference original data that is otherwise nearly impossible to gain access to, relying only on the token's value.[4]

More broadly, cloud protection 'gateways' are made available to prospective cloud customers to install on-premise, in order to protect data at the source, so that only encrypted/tokenised data is processed in-cloud, which is then decrypted or de-tokenised automatically on passing back through the gateway.[5] Such decryption/de-tokenising keys are stored locally in the customer's gateway, with no or limited access from the gateway provider. Thus, providers cannot access anything beyond encrypted or tokenised data, should they attempt, or be required by authorities, to view the customer's data. Gateway providers argue that restrictions on data location are met by processing only tokenized data in-cloud, as the 'real data' remain behind the customer's firewall.[6]

The Prizsm platform is another example of such 'protection gateway' to the cloud, which operates through an algorithm that disaggregates data at bit-level and randomly distributes complementary binary digits to locations across multiple cloud endpoints. Using Prizsm, information is persisted within the platform itself – where the gateway provider claims to have no access to the original information that is disrupted through Prizsm by the data owner– and the data stored in the form of binary digits in any of the connected cloud endpoints cannot be used independently to map back to or recreate the original information that was stored. Accordingly, Prizsm would allow users to comply with local regulations on data protection that operate where the storage provider is located, because restrictions only apply to identifiable personal data, not to non-intelligible data and non-personal data (see below). Secondly, the random allocation of the disrupted binary digits across multiple cloud endpoints increases protection against security breaches and helps preventing and/or avoiding risks related to unauthorized access to cloud data (by the storage provider, hackers, or governments), because in such an event all that can be accessed is a random fraction of binary digits that on its own is unintelligible. Finally, due to the way Prizsm is conceived, in the event of loss of functionality, end of business or corruption, the algorithm would be able to recalculate the missing digits stored in the corrupted cloud endpoint, and thereby allow the user to gain access to the original information.

[4] W Kuan Hon, Christopher Millard, and Jatinder Singh "Control, Security, and Risk in the Cloud" Chapter 2, in C. Millard (ed.) Cloud Computing Law, (2nd edn, OUP 2021), https://global.oup.com/academic/product/cloud-computing-law-9780198716679?lang=en&cc=uk#

[5] Ibid.

[6] Ibid.

An overview of the legislation in force in selected jurisdictions and of the actions in this area of some private companies operating in the sector helps better understanding these issues.

2.1. Spectrum of permissibility in existing legislation

A. EU – General Data Protection Regulation (GDPR 2016)[7]

- **Scope of application**: The Regulation applies to the processing of personal data wholly or partly by automated means and to the processing, other than by automated means, of personal data which form part of a filing system or are intended to form part of a filing system.

  The territorial scope covers the processing of "personal data"[8] by a "controller"[9] or "processor"[10] established in the Union, and by subjects not established in the Union when processing data in the context of activities that are related to: the offering of goods or services (irrespective of payment) and the monitoring of data subjects' behaviour that takes place within the Union (Arts. 2 and 3). Establishment implies the effective and real exercise of activity through stable arrangements. (Recital 22). The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

- **Extra-territoriality**: non-EU based companies that "operate"[11] in the EU need to ensure GDPR compliance, when EU data is involved within the limits of the scope of application set out above, while also adhering to the local laws of the country where they are located. Data processing and/or storage services involve the offering of a good or service, and non-EU established providers would nonetheless be expected to comply with the EU Regulation's prescriptive framework.

- **'Identifiable' v. 'Non-identifiable' personal data**: A relevant distinction is between identifiable and non-identifiable personal data. Under GDPR Art. 4 '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 or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an

[7] 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).
[8] GDPR Article 4 (1): '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 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.
[9] GDPR Article 4 (7): '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.
[10] GDPR Article 4 (8) 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
[11] See GDPR, Art. 3, para. 2.

online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

The principles of data protection should apply to any information concerning an identified or identifiable natural person according to Recital 26 of the Regulation.

It is important to note that "personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms". These include personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs; trade-union membership; genetic data, biometric data processed solely to identify a human being; health-related data; data concerning a person's sex life or sexual orientation.

- **Transfer of personal data to third countries or international organisations** is possible under certain prescribed conditions, for instance on the basis of an adequacy decision by the Commission (Art. 45).[12] When assessing the adequacy of the level of protection by a third country, a territory or one or more specified sectors within a third country, or an international organisation, the Commission takes account of elements such as the rule of law, respect for human rights and fundamental freedoms, relevant legislation, including concerning public security, defence, national security and criminal law and the access of public authorities to personal data, the effective administrative and judicial redress for the data subjects whose personal data are being transferred, the existence and effective functioning of one or more independent supervisory authorities, etc.

  In the absence of an adequacy decision (ex. Art. 45,) personal data can still be transferred to a third country or an international organisation if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available (GDPR, Art. 46).

  The EU Commission considers that UK law provides adequate protection for personal data transferred from the EU to the UK under the EU GDPR, with an exemption on immigration data (see section below on the UK).

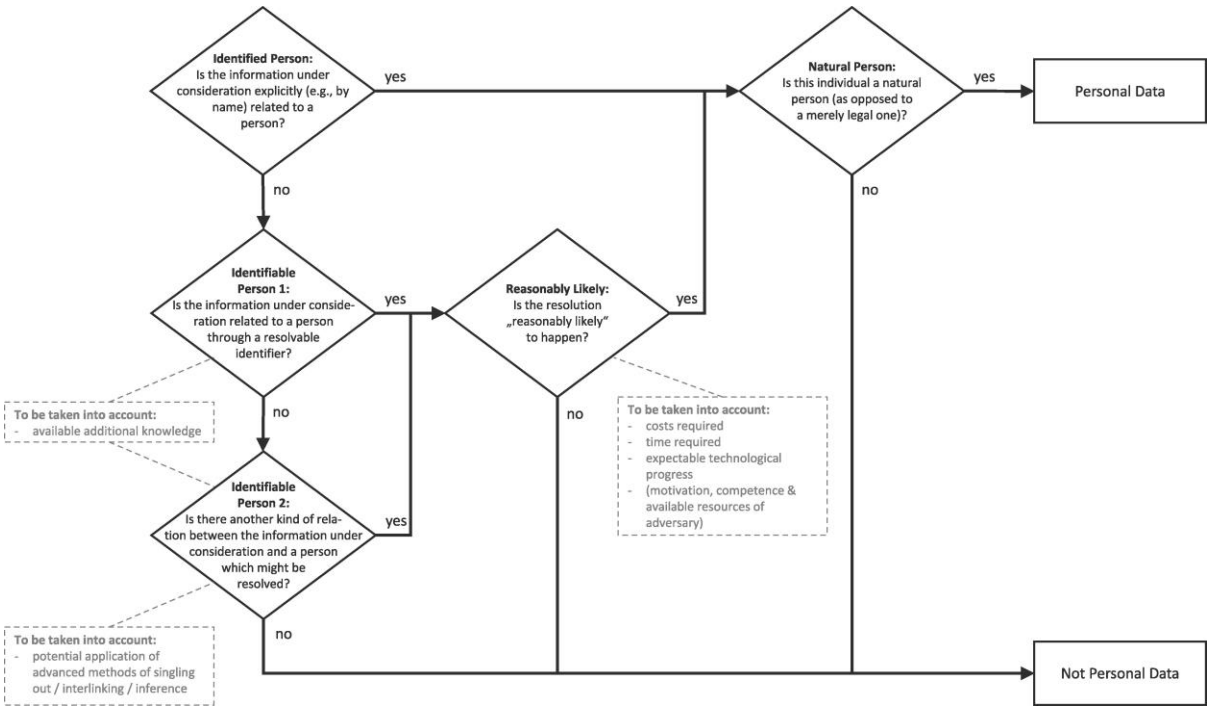
- **Anonymous information** is information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or is no longer identifiable. The principles of data protection do not apply to anonymous information. The Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.

  According to Art. 4 GDPR **'**pseudonymisation**'** means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. Pseudonymisation of personal data can reduce the risks to the data subjects concerned and help controllers and processors meet their data-protection obligations (Recital 28).

[12] This is regulated in GDPR chapter V, Arts. 44 ff.

However, personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments (Recital 26).

The diagram below helps assessing whether the GDPR applies or not to a set of data.



Source: Finck and Pallas, "They who must not be identified—distinguishing personal from non-personal data under the GDPR" (2020) International Data Privacy Law, 2020, Vol. 10, No. 1.

- The EU Regulation only applies to identified or identifiable personal data.
- Prizsm is a UK based company, and the EU commission has issued an adequacy decision regarding the transfer of personal data to the UK (with an exemption on immigration data).
- The EU Regulation effectively prohibits exporting personal data to any cloud provider whose servers are located in countries with weak data protection laws. Based on our understanding of the Prizsm platform and on the explanations provided, the Prizsm algorithm pseudonymises data, to a granular level that makes it nearly-impossible for persons/entities that do not have access to the key to retrieve the original information, taking into account "all objective factors, such as costs, the amount of

time required for identification, and the available technology", as requested by the Regulation. Once personal data is disrupted through the Prizsm algorithm, it becomes un-identifiable and therefore can be safely stored in clouds established in any other jurisdictions, because GDPR limitations only apply to identifiable personal data.

B. UK – Data Protection Act (2018)

- Following Brexit, the **UK Data Protection Act 2018 (DPA)** implements the GDPR, and is currently in effect. There are however some exemptions to the GDPR: Art. 28 provides for a national security and defence modification to Arts. 9 and 32 of the EU GDPR.
- As regards the **territorial scope,** the DPA applies to UK activity and also has extra-territorial effects on companies that offer goods or services involving processing of personal data of UK data subjects.
- **"Data Transfers" to and from the UK**:

  As earlier noted, an EU adequacy decision (under Art. 45 GDPR) considers that UK law provides adequate protection for personal data transferred from the EU to the UK, with an exception on immigration data. It follows that EU personal data can be transferred to the UK freely (except for data related to immigration - subject to review in 2025).

  The Trade and Cooperation Agreement (TCA) between the EU and the UK enables the flow of personal data from the EEA (i.e., EU and Iceland, Liechtenstein, and Norway) to the UK.

  The UK has issued adequacy decisions about the following countries: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Eastern Republic of Uruguay and New Zealand, all EU and EEA member states. UK personal data can be transferred freely to these jurisdictions, subject to some restrictions (subject to review by the end of 2024).

  The US generally does not restrict the export of personal data to other jurisdictions, except the storing of some governmental records and information. This means that data can be transferred freely from the US to the UK, subject to some federal restrictions. Although US policy is less strict, in some occasions, US authorities have taken the position that data may be exported freely but federal regulations still apply to personal data after it leaves the US, as referred to in section C. below. The forthcoming EU-U.S. Data Privacy Framework is expected to facilitate and shed some light on the applicable rules regarding data transfers but is not yet in force.

  Personal information from Australia can only be disclosed to an organization outside of Australia where the entity has taken reasonable steps to ensure that the overseas recipient does not breach the Australian Privacy Principles in relation to the personal information. These are further explained in the Australia section.

  Transfers of UK personal data to third countries are allowed, subject to the appropriate safeguards by the controller or processor. These are often referred to as 'restricted transfers', meaning a transfer of personal data to receivers located outside the UK. If there is no adequacy decision for a country, this does not necessarily foreclose any data transfer

to this country. This can be ensured by using standard contractual clauses (SCCs), or by certification of data processing procedures, subject to national authorities.[13] In the UK, the international data transfer addendum to the EU SCCs for data transfers sets out provisions regarding the current use of the SCCs post-Brexit.

- **UK authorities' access to data**: Under the Investigatory Powers Act 2016, the government has the power to require companies to provide access to data through a targeted equipment interference warrant or a targeted interception warrant. The government can also issue national security notices requiring companies to take specific actions related to data storage or provide data to the government. In addition, the Data Protection Act 2018 and the General Data Protection Regulation (GDPR) set out protections such as the right of data owners to request access to their personal data held by companies. However, these rights may be subject to limitations in cases where the government has a legitimate basis for accessing the data.

- The UK Data Protection Act mirrors the EU GDPR (with minor variances) and only applies to identified or identifiable personal data. When data is anonymised so that it is not possible to identify individuals, it is not considered personal data, and restrictions regarding transfers to third countries would not apply.
- Once disrupted through the Prizsm algorithm, personal data becomes un-identifiable and therefore can be freely and safely stored in clouds established in other jurisdictions, independently of the level of data protection offered in those countries.
- Access to data (personal or other data) by UK authorities only applies to data that originates or is stored in the UK. In different possible scenarios, Prizsm seems to offer a safe and resilient solution. A third country company that stores Prizsm disrupted data with a storage provider in the UK would be protected against interference (UK government seizure order or hacking of data), as the information stored in the UK would only be a fraction of the binary digits composing the original intelligible information. Our understanding is that data would be protected, even if Prizsm Technologies were the subject of a seizure order, as 'Prizsm keys' are tailored and held by each user, but not by Prizsm Technologies itself.

C. Australia – The Privacy Act (1988)

- In Australia, legislation at both the federal and the state/territory level regulates the collection and handling of personal information. The **Privacy Act 1988** is the principal legislation for personal information protection at the Federal Level. This instrument, along with its recent revision, provides a comprehensive set of rules that resemble the EU GDPR. It governs the collection and handling of personal information by agencies of the Commonwealth government and organisations. The term 'organisation' is defined under the Privacy Act to include an individual, a body corporate, a partnership, any other

[13] The EU Standard contractual clauses (SCCs) for international transfers provide standardised and pre-approved model data protection clauses that allow controllers and processors to comply with their GDPR obligations.

unincorporated association or a trust, but excludes 'small businesses', i.e., those with an annual turnover of AUD $3 million or less.

- "**Extra-territoriality**": The Privacy Act has extra-territorial application, and any organisation operating outside of Australia that has "an Australian link" will be required to comply with the Privacy Act. Specific factors that may indicate that an entity is carrying on business activities in Australia include: presence of an agent or agents in Australia; a website that offers goods and services to Australia; an entity that actions purchase orders in Australia or collects personal information from individuals that are physically present in Australia.
- The Privacy Act only governs the **collection and handling of 'personal information'**, which is defined as "information or an opinion about an identified individual or an individual who is reasonably identifiable, whether the information or opinion is true or not, and whether the information or opinion is recorded in a material form or not". A higher level of protection is afforded to information that falls within the definition of 'sensitive information', which includes information or opinion about certain personal attributes such as race, political opinion, religious or philosophical beliefs, membership of an association or union, sexual orientation or criminal record, as well as health information and biometric data.
- Meaning of "**de-identification**": Information that has undergone "an appropriate and robust de-identification process" is not personal information and is therefore not subject to the Privacy Act. An assessment of whether information is personal or de-identified depends on the context, and this assessment does not appear to have been the subject of any judicial consideration in Australia to date.
- The Privacy Act has thirteen 'Australian Privacy Principles' ('the APPs'). They are centred around processing of personal information, setting out standards for the collection, use, disclosure, quality and security of personal information and placing obligations on agencies and organisations subject to the Privacy Act ('APP entities') in respect of access to, and correction of, an individual's own personal information. Notably, APP 11 provides that APP entities that hold personal information must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification or disclosure, and requires APP entities that hold personal information that is no longer needed to take reasonable steps to destroy the information or to ensure that the information is de-identified.
- As in previous analyses of national legislations, Australian authorities hold the power to access privately owned data, in connection with some specific investigation or offence, or national security reasons. Powers in this regard are dispersed throughout several acts, including the Crimes Act 1914 (Cth), the Australian Security Intelligence Organisation Act (ASIO) 1979 (Cth) and the Australian Securities and Investments Commission Act (Cth). Each of these give the government the power to issue a warrant / notice to produce documentation/assets where there is a reasonable suspicion that an offence has been

committed (whether criminal, security risk, corporate offence). The powers under the ASIO Act are the broadest given that they deal with security threats.[14]

- The Australian Privacy Act resembles the EU GDPR and only applies to identified or identifiable personal data. When data is anonymised so that it is not possible to identify individuals, it is not considered personal data and restrictions regarding transfers to third countries would not apply.
- Once disrupted and broken down into a series of binary digits personal data become un-identifiable and therefore can be exported and stored in clouds located in other jurisdictions.

D. United States

- In the United States there is no singular piece of legislation on privacy law at a federal level. Rather, there is a fragmented and sector-specific framework both on a federal and state level.
- **At a Federal level**, the Federal Trade Commission Act (15 U.S. code para.41) seeks to protect consumers from "deceptive practices", including failure to comply with privacy Terms and Conditions set by companies, as well as lack of adequate security of personal information. Among other things, the FTC investigates companies for data breaches and failure to adequately protect consumer information due to weak security measures.
- **Sector-specific laws** include the Children's Online Privacy Protection Act (15 U.S. code para. 6501), prohibiting data collection of children under 13 years of age, without parental consent. Further, there are State-level laws, introducing safeguards on sector-specific data.
- **On a state level**, in recent years there have been developments in privacy legislation and proposals for legislation in order to provide consumers with protection.

  The California Consumer Privacy Act (CCPA) was introduced in 2018 to protect privacy rights of consumers who are California residents, through increased control over personal information. Guarantees include transparency about how personal information is collected, used and shared; the right to delete personal information; and the right to opt-out of the sale or sharing of data. A 2020 amendment enacted the CPRA, which provides for additional guarantees, such as amending inaccurate personal information and the right to limit the use and disclosure of sensitive personal information already collected.

  Several other states have enacted privacy laws, including the Colorado Privacy Act, the Connecticut Data Privacy Act, the Utah Consumer Privacy Act and the Virginia Consumer

[14] Dan Jerker B Svantesson and Rebecca Azzopardi, 'Systematic Government Access to Private-Sector Data in Australia' in Fred H Cate and James X Dempsey (eds), *Bulk Collection: Systematic Government Access to Private-Sector Data* (Oxford University Press 2017) <https://doi.org/10.1093/oso/9780190685515.003.0010> accessed 24 February 2023.

Data Protection Act. These acts provide similar protections, although they are not identical.

The Washington Privacy Act – proposed but not yet in force – would apply to legal entities that conduct business in the State of Washington or that produce products or services that are targeted to residents of Washington.

- In the US, the **government's power to access data stored by companies** is primarily governed by the Electronic Communications Privacy Act (ECPA) and the Foreign Intelligence Surveillance Act (FISA). ECPA sets out the legal procedures for obtaining access to electronic communications and stored electronic data, including emails, and provides a series of protections against the access by governmental agencies to personal information held by third parties. FISA governs the government's collection of foreign intelligence information. The USA Patriot Act has expanded the government's powers to access data for national security purposes. The Fourth Amendment to the US Constitution also protects individuals against unreasonable searches and seizures, which provides some limits on the government's ability to access data without a valid legal basis or court authorization.

- Several pieces of legislation in the US, at federal and state levels, protect private data similarly to the legislation in force in the EU and UK. These laws apply to personal identifiable data. Guarantees are set out for data owners, in the form of transparency requirements, right to deletion from or review of databases. On the other hand, legislation is also in force which might ultimately hinder the privacy and confidentiality of information for the sake of protecting national security and public order.
- Our understanding of the Prizsm Platform is that once disrupted, personal data becomes un-identifiable and therefore can be freely exported and stored in clouds established in different jurisdictions, including in the US. In the event of a seizure of the servers or other interference, the information that is extracted is only a random fraction of the series of binary digits, otherwise not intelligible without the Prizsm algorithm, that is unique to each user.

2.2. Actions of private companies operating in this sector

In addition to the assessment of existing legislation, it is also useful to look at some key data security policies and or solutions of companies that handle/manage data.

- Amazon Web Services (AWS), Inc. is located in the United States, and their affiliated companies are located throughout the world. Depending on the scope of customer interactions with AWS Offerings, personal information may be stored in or accessed from multiple countries, including the United States. When personal information is transferred to other jurisdictions, it is in accordance with their Privacy Notice and as permitted by applicable data protection laws in the relevant jurisdictions. Customers have access and choice regarding their data with options as to how information is being used.

  There is a wide variety of compliance programs for security controls by using encryption protocols and software. For example, Payment Card Industry Data Security Standard (PCI DSS) is used when handling credit card data.

AWS is GDPR compliant. Since Brexit, AWS continues to transfer personal data into and out of AWS regions. Transfer of personal data from the EEA to the UK and vice versa is allowed (adequate level of protection acknowledged), without the need for additional safeguards, including Standard Contractual Clauses (SCCs).

- Some services claim to encrypt data on customers' computers before transfer to the cloud, e.g. SpiderOak SaaS storage, or Mozilla Firefox Sync for browser information storage or synchronization.[15] However, several cloud providers may hold user keys to give providers the technical ability to access customer data (at least if those data are unencrypted), for maintenance or support purposes. Thus, providers can decrypt customer data stored in encrypted form and therefore can have access to intelligible customer data, when necessary (e.g., for technical reasons or when legally required to do so). Dropbox has made such claims,[16] while Apple asserts to use end-to-end encryption for certain sensitive information. This means that only the account owner can access information, and only on devices where he/she is signed into iCloud.[17]
- In addition to self-applied guarantees by data storage companies, encryption or tokenising products that are applied at the source (gateway products) are increasingly offered and designed to be compatible with common cloud services such as AWS, Gmail, Microsoft Office 365 etc., or databases in-cloud, for example Microsoft Azure SQL Database.[18] These are aimed at increasing control over data from customers. The Prizsm platform is one of these tools. End-to-end encryption, where even the provider cannot access customer data, is preferred as in such cases, the provider cannot technically comply with possible law enforcement requests to access the content of customer data.

[15] W Kuan Hon, Christopher Millard, and Jatinder Singh "Control, Security, and Risk in the Cloud" Chapter 2, in C. Millard (ed.) Cloud Computing Law, (2nd edn., OUP 2021), https://global.oup.com/academic/product/cloud-computing-law-9780198716679?lang=en&cc=uk#

[16] Is Dropbox safe to use? - Dropbox Help, https://help.dropbox.com/security/safe-to-use

[17] Apple, 'iCloud security overview', (17 April 2020) https://support.apple.com/en-gb/HT202303.

[18] Ibid.

3. Final considerations relevant to PRIZSM

- Data protection laws in the various jurisdictions assessed introduce restrictions in relation to the processing, storage, management and transfer (including import and export) of identified or identifiable personal data. Such restrictions do not apply when data is anonymised and does not allow identification.
- Our understanding of the Prizsm Platform is that it would allow users to comply with the regulations on data protection that operate where the storage provider is located, because restrictions only apply to identifiable personal data. Prizsm, moreover goes beyond anonymisation of data (both personal and other data), and disaggregates data at the bit level, making it nearly-impossible to retrieve the original information without the 'Prizsm key'.
- The random allocation of the disrupted binary digits across multiple cloud endpoints (through Prizsm) would increase protection against security breaches and would help prevent and/or avoid risks related to unauthorized access to cloud data (by the storage provider, hackers, or governments), because in such an event all that can be accessed is a random fraction of binary digits, unintelligible on its own.
- The Prizsm approach relying on diversification of storage services seems a secure and resilient one that reduces security risks – any damage, loss, or unwarranted access of data stored with a specific storage provider would only affect a random set of binary digits – while also ensuring continued availability of data in the event of loss of functionality, end of business of the storage platform or data corruption. Based on our understanding of the way Prizsm is conceived, the algorithm would be able to recalculate the missing digits stored in the corrupted cloud endpoint, and thereby allow the user to gain access to the original information, provided that the key is available which is something only data owners would have.
- On the contrary, any attempt to hack or otherwise access data (including by law enforcement under powers granted through legislation) would only reach a series of disrupted binary digits which on their own are unintelligible. The storage provider would not be in a technical position to access or provide to authorities intelligible data because no such intelligible data will be stored with any one storage provider.
- Despite the safe solution for multi-cloud digital information storage offered by Prizsm, Prizsm platform users, as the main controllers of the Platform and its keys must invest in security measures at their end.

Bibliography

Advisors SC, 'Anonymization and GDPR Compliance; an Overview' (GDPR Summary, 21 July 2020) <https://www.gdprsummary.com/anonymization-and-gdpr/>

Akhlaghpour S and others, 'Learning from Enforcement Cases to Manage GDPR Risks.' (2021) 20 MIS Quarterly Executive 199 <https://proxy.umo.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=152709663&site=ehost-live&scope=site>

Angela Pottter and others, 'Comparing Privacy Laws: GDPR v. Australian Privacy Act' (OneTrust DataGuidance 2017) <https://www.dataguidance.com/sites/default/files/gdpr_v_australia.pdf>

Bennett S, 'Gdpr: Change to European Privacy Laws and Its Impact on Australian Businesses' (2018) 70 Governance Directions 85 <https://search.informit.org/doi/10.3316/informit.481655065059932> accessed 23 November 2022

Bhatt DA, 'Data Sovereignty- the Quintessential Model for the New World Order' [2021] Issue of ILI Review <https://papers.ssrn.com/abstract=3935134> accessed 24 February 2023

Bradshaw S, Millard C and Walden I, 'Contracts for Clouds: Comparison and Analysis of the Terms and Conditions of Cloud Computing Services*' (2011) 19 International Journal of Law and Information Technology 187 <https://doi.org/10.1093/ijlit/ear005>

Chander A and Le UP, 'Breaking the Web: Data Localization vs. the Global Internet' [2014] Emory Law Journal UC Davis Legal Studies Research Paper No. 378 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2407858>

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 2020) <https://papers.ssrn.com/abstract=3748098>

Cradduck L, Stevens S and Cowan M, 'Data Sharing, International Property Practices and the GDPR: Communicating with Your Consumers' (2021) 39 Property Management 22 <https://doi.org/10.1108/PM-05-2020-0033> accessed 23 November 2022

Das Chaudhury R and Choe C, 'Digital Privacy: GDPR and Its Lessons for Australia' [2022] Available at SSRN 4219468 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4219468>

Diker Vanberg A, 'The Right to Data Portability in the GDPR: What Lessons Can Be Learned from the EU Experience?' (2018) 21 Journal of Internet Law 12 <http://gala.gre.ac.uk/id/eprint/24255/>

Eckstein L and others, 'Australia: Regulating Genomic Data Sharing to Promote Public Trust' (2018) 137 Human Genetics 583 <https://link.springer.com/article/10.1007/s00439-018-1914-z>

F. Paul Pittman, Kyle Levenberg, and Shira Shamir, 'Relevant Legislation and Competent Authorities', Data Protection Laws and Regulations USA 2022 (Global Legal Group 2022) <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa>

Feld EL, 'United States Data Privacy Law: The Domino Effect after the GDPR Mini-Symposium on Comprehensive Data Privacy Reform Legislation in the United States' (2020) 24 North Carolina Banking Institute 481 <https://heinonline.org/HOL/P?h=hein.journals/ncbj24&i=505>

Finck M and Pallas F, 'They Who Must Not Be Identified—Distinguishing Personal from Non-Personal Data under the GDPR' (2020) 10 International Data Privacy Law 11 <https://doi.org/10.1093/idpl/ipz026> accessed 11 March 2022

Gladstone MH, 'GDPR in United State Litigation through Summer 2020: GDPR-Subject Companies Must Produce' (2020) 87 Defense Counsel Journal 1 <https://heinonline.org/HOL/P?h=hein.journals/defcon87&i=251>

Goddard M, 'The EU General Data Protection Regulation (GDPR): European Regulation That Has a Global Impact' (2017) 59 International Journal of Market Research 703 <https://journals.sagepub.com/doi/pdf/10.2501/IJMR-2017-050>

Group GL, 'International Comparative Legal Guides' (International Comparative Legal Guides International Business Reports) <https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa> accessed 10 November 2022

Hon WK, Millard C and Walden I, 'The Problem of "Personal Data" in Cloud Computing: What Information Is Regulated?—The Cloud of Unknowing *' (2011) 1 International Data Privacy Law 211 <https://doi.org/10.1093/idpl/ipr018>

Jones ML and Kaminski ME, 'An American's Guide to the GDPR' (2020) 98 Denv. L. Rev. 93 <https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/denlr98&section=5>

Kamarinou D, Millard C and Turton F, '294Responsibilities of Controllers and Processors of Personal Data in Clouds' in Christopher Millard (ed), Cloud Computing Law (Oxford University Press 2021) <https://doi.org/10.1093/oso/9780198716662.003.0009> accessed 24 February 2023

Koch R, 'What Is Considered Personal Data under the EU GDPR?' (GDPR.eu, 1 February 2019) <https://gdpr.eu/eu-gdpr-personal-data/> accessed 1 December 2022

Kulbeth M, 'Does the GDPR Apply in the USA?' (SixFifty, 9 March 2020) <https://www.sixfifty.com/blog/does-the-gdpr-apply-in-the-usa/> accessed 10 November 2022

Li H, Yu L and He W, 'The Impact of GDPR on Global Technology Development' (2019) 22 Journal of Global Information Technology Management <https://www.tandfonline.com/doi/abs/10.1080/1097198X.2019.1569186>

Lundstedt L, 'International Jurisdiction over Crossborder Private Enforcement Actions under the GDPR' [2018] Faculty of Law, Stockholm University Research Paper 50 <https://dx.doi.org/10.2139/ssrn.3159854>

Meese J, Jagasia P and Arvanitakis J, 'Citizen or Consumer? Contrasting Australia and Europe's Data Protection Policies' (2019) 8 Internet Policy Review 1 <https://www.econstor.eu/handle/10419/214076>

Mitchell AD and Samlidis T, 'Cloud Services and Government Digital Sovereignty in Australia and Beyond' (2022) 29 International Journal of Law and Information Technology 364 <https://doi.org/10.1093/ijlit/eaac003>

Moerel L and Timmers P, 'Reflections on Digital Sovereignty' [2021] EU Cyber Direct, Research in Focus series

Pastor N, 'Is This Personal Data? The ICO Updates Its Guidance on Anonymisation.' (Fieldfisher, 4 June 2021) <https://www.fieldfisher.com/en/services/privacy-security-and-information/privacy-security-and-information-law-blog/is-this-personal-data-the-ico-updates-its-guidance>

Peloquin D and others, 'Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data' (2020) 28 European Journal of Human Genetics 697 <https://doi.org/10.1038/s41431-020-0596-x>

Politis K, 'GDPR – Impact on Australian Businesses' (KHQ Lawyers, 6 June 2018) <https://www.khq.com.au/legal-blog/gdpr-australian-businesses/> accessed 11 November 2022

Pop C, 'EU vs US: What Are the Differences Between Their Data Privacy Laws?' (Endpoint Protector Blog, 27 September 2022) <https://www.endpointprotector.com/blog/eu-vs-us-what-are-the-differences-between-their-data-privacy-laws> accessed 10 November 2022

Rauhofer J and Bowden C, 'Protecting Their Own: Fundamental Rights Implications for EU Data Sovereignty in the Cloud' [2013] University of Edinburgh, School of Law <https://www.research.ed.ac.uk/en/publications/protecting-their-own-fundamental-rights-implications-for-eu-data-> accessed 24 February 2023

Reed C, 'Information Ownership in the Cloud', Cloud Computing Law (Oxford University Press 2021) <https://doi.org/10.1093/oso/9780198716662.003.0005>

Revolidis I, 'Judicial Jurisdiction over Internet Privacy Violations and the GDPR: A Case of Privacy Tourism' (2017) 11 Masaryk U. J.L. & Tech. 7 <https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/mujlt11&section=5>

Ryngaert C and Taylor M, 'The GDPR as Global Data Protection Regulation?' (2020) 114 AJIL Unbound 5 <https://www.cambridge.org/core/article/gdpr-as-global-data-protection-regulation/CB416FF11457C21B02C0D1DA7BE8E688>

Schildhaus A, 'EU's General Data Protection Regulation GDPR: Key Provisions and Best Practices Articles' (2017) 46 Int'l L. News 12 <https://heinonline.org/HOL/Page?handle=hein.journals/inrnlwnw46&id=52&collection=usjournals&index=>

Svantesson DJB and Azzopardi R, 'Systematic Government Access to Private-Sector Data in Australia' in Fred H Cate and James X Dempsey (eds), Bulk Collection: Systematic Government Access to Private-Sector Data (Oxford University Press 2017) <https://doi.org/10.1093/oso/9780190685515.003.0010> accessed 24 February 2023

Vaile D and others, Data Sovereignty and the Cloud: A Board and Executive Officer's Guide (SSRN 2015) <https://books.google.co.uk/books?id=9JEQzwEACAAJ>

Vokinger KN, Stekhoven DJ and Krauthammer M, 'Lost in Anonymization—A Data Anonymization Reference Classification Merging Legal and Technical Considerations' (2020) 48 Journal of Law, Medicine & Ethics 228 <https://www.cambridge.org/core/journals/journal-of-law-medicine-and-ethics/article/abs/lost-in-anonymization-a-data-anonymization-reference-classification-merging-legal-and-technical-considerations/B3157FF1EBF29208EAB7033932990720>

Wagner J and Benecke A, 'National Legislation within the Framework of the GDPR' (2016) 2 Eur. Data Prot. L. Rev. 353 <https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/edpl2&section=60>

Watts D and Casanovas P, 'Australian Entities and the EU General Data Protection Regulation (GDPR)' [2018] Australian Government OAIC <https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation> accessed 23 November 2022

——, 'Privacy and Data Protection in Australia: A Critical Overview', W3C Workshop on Privacy and Linked Data (World Wide Web Consortium 2019) <https://ddd.uab.cat/record/243649>

Williams S, 'GDPR—Not Just an EU Regulation?' (2018) 19 The Lancet Oncology e508

Woods AK, 'Litigating Data Sovereignty' (2018) 128 Yale Law Journal <https://papers.ssrn.com/abstract=3256422> accessed 24 February 2023

Ziegler S, Evequoz E and Huamani AMP, 'The Impact of the European General Data Protection Regulation (GDPR) on Future Data Business Models: Toward a New Paradigm and Business Opportunities' 201 <https://doi.org/10.1007/978-3-319-96902-2_8>

California Consumer Privacy Act (CCPA) 2018

General Data Protection Regulation (GDPR)

Charles Clore House
17 Russell Square
London WC1B 5JP

T 020 7862 5151
F 020 7862 5152
E info@biicl.org

www.biicl.org

A company limited by guarantee
Registered in England No. 615025
Registered Charity No. 209425

British Institute of
International and
Comparative Law