THE INTERNATIONAL DEVELOPMENT OF ONLINE PRIVACY PROTECTION AND UNIVERSAL CORE PRIVACY RIGHTS IN THE PUBLIC INTEREST: A CONTENT ANALYSIS AND A COMPARATIVE INTERNATIONAL STUDY

by

Tyra Jane Chantson

14320275

Submitted in partial fulfilment of the requirements for the degree

LLM in International Air, Space and Telecommunications Law

in the

FACULTY OF LAW

at the

UNIVERSITY OF PRETORIA

Date

2018 October

Supervisor : Professor S Hobe

ABSTRACT

Privacy is considered as an important human right, and should accordingly be protected by States. Given the lack of a uniform and binding international order for cyber security and data protection, privacy in the online environment is often vulnerable to abuse by a variety of actors, including private international entities such as Facebook and Google. Data protection laws differ from state to state, which may result in inconsistent practices being carried out by international companies. There is a call for States to develop a uniform international order to regulate the internet and information and communications technology law. Thus the main question of this study is whether there exists an international standard of data protection that gives effect to online privacy protection, and which can be enforced. Such an international standard would be enforceable if it has become a rule of customary international law, as prescribed by the Statute of the International Court of Justice.

The basic privacy protection standards provided by international organisations are often non-binding and are understood and implemented differently across States. Therefore, a comparison is drawn between these basic privacy protection standards provided by international organisations, as well as the various legal frameworks of States pertaining to online privacy protection or data protection. This exercise establishes that there may be a customary international rule that recognises online privacy protection and prescribes a certain standard of data protection.

This study further investigates how an international standard can directly bind both states and private entities in a dynamic legal field such as internet law. Enforcement of online privacy may require one to look beyond the traditional division between states and private entities in international law as the internet goes beyond territorial jurisdiction.

University of Pretoria

Declaration of originality

This document must be signed and submitted with every essay, report, project, assignment, mini-dissertation, dissertation and/or thesis

.

Full names of student:
TYRA JANE CHANTSON
.....

Student number: ……14320275…….....

Declaration

1. I understand what plagiarism is and am aware of the University's policy in this regard.

2. I declare that this ……MINI-DISSERTATION…… (e.g. essay, report, project, assignment, mini-dissertation, dissertation, thesis, etc) is my own original work. Where other people's work has been used (either from a printed source, Internet or any other source), this has been properly acknowledged and referenced in accordance with departmental requirements.

3. I have not used work previously produced by another student or any other person to hand in as my own.

4. I have not allowed, and will not allow, anyone to copy my work with the intention of passing it off as his or her own work.

Signature of student:...…….....

Signature of supervisor:…….....……..

ACKNOWLEDGMENTS

With sincere thanks to

Professor S Hobe for his mentorship.

Friends, family and colleagues for their moral support.

My mother, Janine, for her endless love and support, enabling to complete this dissertation.

Table of Contents

CHAPTER 1 INTRODUCTION

1.1 Background

The continuous exponential growth of the digital world coupled with the rise of potentially invasive applications or systems, such as location based services or web-tracking applications, as well as the lack of a coherent, uniform and binding international order for cyber security and data protection, leaves room for the undermining of online privacy rights, especially by private international entities such as Facebook and Google. The internet, a globally connected network system, involves many role players, both public and private, and remains heavily unregulated. Data and online privacy protection laws differ from state to state, which may result in inconsistent practices being carried out by international companies. There is a call for States to develop a uniform international order to regulate the internet and cyberspace.

1.2 Aims of the study

This study aims to contribute to the legal discourse by clarifying the position of online privacy in international law. In doing so, the study seeks to establish whether an international standard comprising of internationally agreed-upon principles on information privacy protection exists, and if so, whether the standard has formed a rule of customary international law.

The study considers recent developments that extend the fundamental right to privacy, as embodied in the Universal Declaration of Human Rights and other international and regional treaties, to online activity in our digital age. The study also investigates ways in which an international standard could be effectively enforced, and bind both states and private entities.

1.3 Methodology

A desktop research methodology will be employed throughout this study. This entails textual analysis and review of existing literature.

Firstly, the meaning of privacy, online privacy and data protection shall be discussed with reference to existing literature, as well as to relevant provisions in international

treaties. This involves a black letter or doctrinal analysis. Secondly, the core principles of privacy and data protection as provided by authors will be analysed with reference to the text and content of existing international and regional instruments. This entails a textual and comparative analysis of the relevant instruments to establish the presence of the core principles of privacy and data protection.

A conceptual analysis of existing laws in individual states will be then be followed to determine whether a state recognises the right to privacy and data protection, and whether the legal framework of a state provides for online privacy protection. Then a comparative legal research methodology between the legal frameworks of the States recorded on the DLA Piper database will be adopted to establish similarities between the online privacy protections afforded in these States.

The study will then investigate and analyse whether the core data protection principles have become a customary international standard. The information presented in the sections above, existing literature, as well as international treaty and case law, will aid this analysis.

The final part of the study entails a normative approach in analysing the text of secondary sources, such as books and articles, to investigate effective means of implementing an international standard that is binding worldwide. A critical approach of existing literature and the traditional division between states and private entities will be adopted.

CHAPTER 2 CONCEPT OF ONLINE PRIVACY

2.1 The definition of privacy

Various authors agree that there is no set definition for privacy; the meaning of privacy differs from State to State.[1] Western traditions tend to link privacy to individual autonomy. Accordingly, privacy must be protected by law, whether by limiting government interference, or by creating conditions for individual autonomy.[2] Privacy has been described as being fundamental to preserving personal sense of self and to developing relationships with others.[3] The right to privacy is recognised as fundamental human right in international law, and an important facet of human dignity.[4]

The report, Privacy and Human Rights 2006, published by the Electronic Privacy Information Center and Privacy International defines privacy and separates it into four concepts:[5]

> **Information privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information, and medical and government records. It is also known as "data protection";
> **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as genetic tests, drug testing and cavity searches;
> **Privacy of communications,** which covers the security and privacy of mail, telephones, e-mail and other forms of communication; and
> **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks.

The protection of these aspects can often be found in local laws and constitutions. The majority of states in the international community have included the right to privacy as fundamental human right in their national constitutions. Furthermore, these aspects can be found in international treaties, which will be discussed below. Although the right to privacy, as enshrined in international treaties, is recognised as a fundamental human right, it is not absolute.

---

1 D Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29(1) Melbourne University Law Review 136-138, 142-144.

2 Idem at 168-169.

3 A Rengel, 'Privacy as an International Human Right and the Right to Obscurity in Cyberspace' (2014) 2(2) Groningen Journal of International Law 39, 40, 52.

4 Idem at 42, 52-53.

5 M Rotenberg and A Knight, Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments (1st edn, Electronic Privacy Information Center, Washington and Privacy International, London 2007).

2.2 The right to privacy in treaties

The right to privacy is explicitly protected in the Universal Declaration of Human Rights (UDHR),[6] and the International Covenant on Civil and Political Rights (ICCPR).[7] In terms of Article 12 of the UDHR, every person has the right to have his or her 'privacy, family, home or correspondence' protected by law against arbitrary interference, and to be protected against 'attacks upon his [or her] honour and reputation.'[8] A similar provision is contained in Article 17 of the ICCPR.

The right to privacy is recognised in numerous regional treaties as well. Article 8(1) of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) recognises that every person has the right to respect for his or her private and family life, home and correspondence.[9] A public authority may not interfere with this right unless such interference is lawful, necessary and in the public interest.[10] The Charter of Fundamental Rights of the European Union explicitly recognises both the right to privacy,[11] and the right to protection of personal data.[12]

Article 12 of the UDHR is echoed in Article V, IX and X of the American Declaration of the Rights and Duties of Man.[13] The right to privacy is similarly protected in Article 11 of the American Convention on Human Rights.[14]

Although the African Charter on Human and Peoples' Rights does not specifically and explicitly refer to the right to privacy, Article 5 of the Charter can be read to encompass privacy rights.[15]

---

6 Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III) (UDHR) art 12 read with art 3.

7 International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) art 17.

8 UDHR art 12.

9 European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) art 8(1).

10 ECHR art 8(2).

11 Charter of Fundamental Rights of the European Union [2012] OJ C 326/02 (EU Charter of Fundamental Rights), art 7.

12 EU Charter of Fundamental Rights, art 8.

13 American Declaration of the Rights and Duties of Man, OAS Res XXX adopted by the Ninth International Conference of American States (1948) reprinted in Basic Documents Pertaining to Human Rights in the Inter-American System OEA/Ser L V /II.82 Doc 6 Rev 1 at 17 (1992) art V, IX and X.

14 American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) (1969) 1144 UNTS 123 art 11.

15 African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21

The United Nations General Assembly recognises the importance of online privacy in the modern era, and consequently signed a non-binding resolution on the right to privacy in the digital age.[16]

2.3 The relationship between privacy and data protection

The relationship between the privacy and data protection is a topic of discussion amongst authors and commentators. Though various and differing arguments have been submitted to this end, it appears that there is a general consensus that privacy and data protection are separate and distinct concepts.

De Hert and Gutwirth describes privacy as a 'tool of opacity' and data protections as a 'tool of transparency'.[17] Privacy acts as a 'tool of opacity' in that it protects the autonomy, liberty and private life of the individual against interference by the state and private actors.[18] Consequently, privacy relates to the management of personal information.[19] According to de Hert and Gutwirth, privacy protects the individual against unlawful and excessive use of power, while data protection prescribes the conditions and rules for the legitimate processing of data.[20] Data protection thus acts as a 'tool of transparency', and provides individuals with a level of control over their data and the way in which their data is used.[21]

Bygrave emphasises that privacy and data protection are separate constructs that both exist independently.[22] Bygrave contends that data protection assists in the realisation of privacy rights.[23] However, the scope of data protection extends beyond the privacy.[24] The right to data protection provides individuals with more control over

---

October 1986) (1982) 21 ILM 58, art 5.

16 United Nations General Assembly Resolution 68/167 (18 December 2013).

17 P De Hert and S Gutwirth, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E Claes, A Duff and S Gutwirth (eds.), *Privacy and the Criminal Law* (Intersentia, 2006) 69-73.

18 Ibid.

19 Ibid.

20 Idem at 73-76.

21 Ibid.

22 L Bygrave, 'The Place of Privacy in Data Protection Law' (2001) University of New South Wales Law Journal 277-283.

23 Ibid; A Forde, 'The Conceptual Relationship between Privacy and Data Protection' (2016) 1 Cambridge Law Review 146.

24 Ibid; N Purtova, 'Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights' (2010) 28(2) Netherlands Quarterly of Human Rights 182.

more personal data than the right to privacy.[25] Lynskey affirms that this heightened control serves two key purposes: firstly, 'it promotes the right to personality of individuals through informational self-determination'; and secondly, 'it reduces the information and power asymmetries which can have a negative impact on individual autonomy'.[26]

2.4 The meaning of online privacy

Online privacy is known as internet privacy.[27] The English Oxford Living Dictionaries defines 'online' as an adjective relating to an activity or service 'available on or performed using the Internet or other computer network'.[28] Online privacy thus concerns the right to privacy in respect of internet activity and personal information of the data subject provided over the internet. Online privacy concerns the privacy of all persons around the world who use the internet, and therefore online consumer privacy should not be limited to policies in the private sphere only. Caudill & Murphy correctly emphasise that online consumer privacy is a public policy matter, and that uniform international principles to protect online privacy should be developed accordingly.[29]

Online privacy protection includes 'techniques, factors and technologies used to protect private and sensitive data, [personal] preferences and communications'.[30]
As indicated by DLA Piper, online privacy protection generally encompasses location data, traffic data, cookies and the storage of specific information.[31]

---

25 O Lynskey, 'Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order' (2014) 63(3) International and Comparative Law Quarterly 569-597; Forde (n 23) 147.

26 Ibid.

27 Dynamix Solutions, 'What is Internet Privacy and What Does Privacy Mean to You?' (*Dynamix Solutions*, 14 April 2017) <https://www.dynamixsolutions.com/what-is-internet-privacy-and-what-does-privacy-mean-to-you/> accessed 6 June 2018.

28 English Oxford Living Dictionaries, 'Definition of *online*' (*Oxford University Press*, 2018) <https://en.oxforddictionaries.com/definition/online> accessed 20 June 2018.

29 EM Caudill and PE Murphy, 'Consumer Online Privacy: Legal and Ethical Issues' (2009) 19(1) Journal of Public Policy & Marketing 7,16.

30 Dynamix Solutions (n 27).

31 'Data Protection Laws of the World: Full Handbook' (DLA Piper, October 2018) <https://www.dlapiperdataprotection.com/index.html>accessed 11 October 2018.

2.4.1 Location based services

The International Association of Privacy Professionals (IAPP) defines location based services as 'services that utilise information about location to deliver, in various contexts, a wide array of applications and services, including social networking, gaming and entertainment.'[32] These services typically rely on satellite-based navigation systems, like the Global Positioning System (GPS), or similar technologies in which geolocation is used to identify the geographic location of an object, such as a mobile or an internet-connected computer terminal.[33]

2.4.2 Traffic data

The IAPP defines 'traffic data' as 'any data processed for the purpose of the conveyance of a communication on an Electronic Communications Network or for the billing thereof.'[34] This includes information about the type, format, time, duration, origin, destination, routing, protocol used and the originating and terminating network of a communication.[35]

2.4.3 Cookies

'Cookies' are defined by the IAPP as small text files stored on a device that may later be retrieved by a web server.[36] Cookies allow web servers to keep track of the end user's browser activities, and connect individual web requests into a session.[37] Cookies may be referred to as 'first party cookies' (if they are placed by the visited website) or 'third party cookies' (if they are placed by a party other than the visited website).[38]

2.5 Threats to online privacy

Caudill & Murphy accept that the infringement of privacy depends on whether consumers have control over the extent of personal information collected, and

---

32 International Association of Privacy Professionals, 'Glossary of Privacy Terms' (IAPP, 2018) <https://iapp.org/resources/glossary/> accessed 10 May 2018.
33 Ibid.
34 Ibid.
35 Ibid.
36 Ibid.
37 Ibid.
38 Ibid.

whether consumers have knowledge of their personal information being collected and used.[39] Past studies reveal that individuals are often unaware of what information has been collected about them as well as the purpose for which their information is being collected.[40] Rachovitsa stresses that the online privacy of consumers can be abused through invasive digital tracking.[41] Mayer & Mitchell indicate that third-party web tracking is a great concern for consumer privacy as consumers often do not consent to such tracking. This situation arises when a user voluntarily visits a first-party website, and a third-party website is permitted by the first-party website to learn about that user.[42] Most activity online leaves a digital trail which can be collected, manipulated and be used to monitor individuals without individuals being able to control the use of their data.[43] Without legal or technological protection, individuals' right to privacy can easily be invaded and infringed over the internet.

39 Caudill and Murphy (n 29) 8.

40 Ibid; Rengel (n 3) 42-50.

41 A Rachovitsa, 'Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue' (2016) 24 International Journal of Law and Information Technology 374-375.

42 JR Mayer and JC Mitchell, 'Third-Party Web Tracking: Policy and Technology (2012 IEEE Synopsis on Security and Privacy, San Francisco, May 2012) 413.

43 Rengel (n 3) 42-44.

CHAPTER 3 ONLINE PRIVACY PROTECTION IN INTERNATIONAL LAW

3.1 Introduction

The fundamental right to privacy both offline and online has been recognised by the international community. At present, there is no single, coherent and uniform order or standard that regulates online privacy and is binding on an international level. Various international organisations have, however, provided guidelines on basic privacy and data protection.

The Organisation for Economic Co-Operation and Development (OECD) first published Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data in 1980, which contains the basic eight principles for the protection of privacy on a national level.[44] These principles are widely referred to, and provided the foundations for the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.[45] Though the APEC Privacy Framework was founded on the OECD Guidelines, its similar information privacy principles are formed quite differently, with greater emphasis on the importance of global commerce and the free flow of information rather than the right to privacy *per se*.[46] The APEC Privacy Framework offers guidance to member states in 'developing data privacy approaches that would optimise the balance between privacy protection and cross-border data flows'.[47] Both the OECD Guidelines and the APEC Privacy Framework are non-binding on member states.

Two regional instruments exist in the Europe that are relevant to this discussion, namely, the European Union General Data Protection Regulation (GDPR),[48] and the

---

44 Organisation for Economic Co-Operation and Development (OECD), 'Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (adopted 23 September 1980, amended 11 July 2013) OECD/LEGAL/0188 (OECD Guidelines) part 2 of the annex.

45 Asia-Pacific Economic Cooperation (APEC) 'APEC Privacy Framework' (published by APEC in August 2017) (2015) APEC #217-CT-01.9.

46 JG Tan, 'A Comparative Study of the APEC Privacy Framework –A New Voice in the Data Protection Dialogue?' (2008) 3 Asian Journal of Comparative Law 3.

47 ER Cooper and AC Raul, 'APEC Overview' in AC Raul (ed), *The Privacy, Data Protection and Cybersecurity Law Review* (4th edn, Law Business Research Ltd, London 2017) 27.

48 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on

Council of Europe Convention for the Protection of the Individuals with regard to Automatic Processing of Personal Data (CoE Convention).[49] The CoE Convention is not a self-executing instrument, and parties must first sign and ratify the instrument into their national law for it to be legally binding upon them. It must be noted the CoE Convention applies only to automated data processing. The GDPR, on the other hand, is a self-executing document and is automatically binding upon all member states of the European Union (EU). The GDPR replaced the EU Data Protection Directive 95/46/EC, and is fully operation as of May 2018.

The African Union (AU) adopted the African Union Convention on Cyber Security and Personal Data Protection (AU Convention) in June of 2014.[50] This Convention also envisages a basic standard of data protection. This Convention, however, has not yet entered into force. Though this Convention has not yet entered into force, it is relevant to this study as African member states are encouraged to follow this Convention over other African model regulations.

Notwithstanding differences in language, legal traditions, and cultural and social values, authors and commentators have reached a general agreement on the basic content and core principles that data protection legislation should encompass.[51] These core principles of data protection can be found, in one form or another, in all successful data protection laws.[52] Bygrave identifies eight core principles that effective data protection laws apply to the processing of personal data, namely fair and lawful processing; minimality; purpose specification; information quality; data subject participation and control; disclosure limitation; information security; and data sensitivity.[53] Roos adds openness and transparency, and accountability as separate principles.[54] The privacy and data protection standards as laid down in the OECD

---

the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2016 L 119/1.

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

50 Africa Union Convention on Cyber Security and Personal Data Protection (adopted by the Twenty-third Ordinary Session of the Assembly on 27 June 2014, Malabo, Equatorial Guinea, not yet in force).

51 A Roos, 'Core principles of data protection law' (2006) 39(1) The Comparative and International Law Journal of Southern Africa 107.

52 Ibid.

53 L Bygrave, 'An international data protection stocktake @ 2000, Part 2: core principles of data protection instruments' (2001) 7 Privacy Law & Policy Reporter 169-178.

54 Roos (n 51) 126-129.

Guidelines, APEC Privacy Framework, the GDPR, the CoE Convention, and the AU Convention will now be considered in light of the core principles of data protection.

3.2 Core principles of data protection

3.2.1 Fair and lawful processing

First and foremost, personal data should be processed fairly and lawfully.[55] In order for data processing to be lawful, certain conditions that justify the processing must be met. According to Bygrave, fairness entails that data controllers should consider the interests and reasonable expectations of data subjects; data processing should not unreasonably interfere with the privacy of a data subject; persons should not be unduly pressured to provide data about themselves; personal data should be collected directly from the data subject so as to facilitate transparent data processing; and data acquired for one purpose may not without the data subject's consent be used for another unrelated purpose which the data subject would not reasonably anticipate.[56]

The 'Collection Limitation Principle' contained in both the OECD Guidelines and the APEC Privacy Framework reflects this principle and includes an additional criterion that personal data be acquired with the knowledge or consent of the data subject where appropriate.[57]

The principle of fair and lawful processing, in its basic form, is set out in the CoE Convention,[58] and in Article 5(1)(a) of the GDPR. The GDPR explicitly imposes certain conditions for the lawful processing of personal data in Article 6(1), including, but not limited to, the requirement of consent by the data subject.[59]

55 Bygrave (n 53) 'An international data protection stocktake @ 2000, Part 2' 169-171.
56 Ibid.
57 OECD Guidelines, par 7; APEC Privacy Framework, par 24.
58 Council of Europe Convention 108, art 5(a) 'Quality of data'.
59 General Data Protection Regulation, art 6(1)(a).

The AU Convention includes the principle of lawful and fair processing in its Basic Principles Governing the Processing of Personal Data,[60] but lists consent as a separate principle for the legitimacy of the processing of personal data.[61]

3.2.2 Minimality

The principle of minimality can also be referred to as 'non-excessiveness' or 'proportionality'.[62] Bygrave states that in terms of the principle of minimality, the amount of personal data collected 'should be limited to what is relevant and necessary to achieve the purpose(s) for which the data are gathered and processed'.[63] This is reflected in the GDPR,[64] the CoE Convention,[65] the APEC Privacy Framework,[66] and the AU Convention.[67]

Roos states that the application of the principle of minimality infers that personal data should be destroyed or conveyed in an anonymous form once the data are no longer required for the purpose for which they were initially collected.[68] This aspect appears to only have been explicitly incorporated in the GDPR,[69] the CoE Convention,[70] and the AU Convention.[71]

The OECD Guidelines fails to make specific provisions for the principle of minimality and for the destruction or anonymization of personal data after a certain time.[72] The OECD Guidelines merely states that 'there should be limits to the collection of personal data'.[73]

---

60 AU Convention, art 13 (basic principles governing the processing of personal data), principle 2.

61 AU Convention art 13, principle 1. In the same paragraph, the conditions in which consent may be waived are listed. These conditions are similar to the conditions prescribed in Article 6(1)(a) to (f) of the GDPR.

62 Bygrave (n 53) 171, 172.

63 Ibid.

64 General Data Protection Regulation, art 5(1)(c).

65 Council of Europe Convention 108, art 5(c).

66 APEC Privacy Framework, par 24.

67 AU Convention, art 13, principle 3(b).

68 Roos (n 51) 114; Bygrave (n 53) 170, 171.

69 General Data Protection Regulation, art 5(1)(e)

70 Council of Europe Convention 108, art 5(e)

71 AU Convention, art 13, principle 3(c) and (d)

72 Bygrave (n 53) 171, 172.

73 OECD Guidelines, par 7 'Collection limitation principle'.

3.2.3 Purpose specification

The collection of personal data should be limited to specified, lawful or legitimate purposes, and personal data shall not be further processed in a way that is incompatible with those purposes specified.[74] This principle is mirrored in the GDPR,[75] the CoE Convention,[76] and the AU Convention.[77]

The 'Purpose Specification' principle in the OECD Guidelines reflects this principle but indicates further that data subjects should be notified of these specified purposes prior to the collection of their personal data, as well as of any changes to the initial purposes.[78]

The principle of purpose specification is not listed as a separate principle under the APEC Privacy Information Principles, but can be inferred by the notice principle read together with the choice principle and the use of personal information principle.

According to the 'Notice' principle, data subjects should be notified of, among other things, the purposes for which personal information is collected prior to or at the time of collection of their personal data, or if such is not practical, as soon as it is practicable.[79] The 'Use of Personal Information' principle limits the use of personal data collected 'to fulfilling the purposes of collection and other compatible or related purposes'.[80]

3.2.4 Information quality

Personal data should be valid and relevant in respect of what they are intended to describe, and accurate and up to date with regard to the purposes for which they will be processed.[81] In essence, data controllers must make certain that personal data is relevant, complete, accurate and up to date.[82]

---

74 Bygrave (n 53) 172, 173; Roos (n 51) 113, 114.

75 General Data Protection Regulation, art 5(1)(b). This provision also includes circumstances where the further processing for archiving purposes are not considered incompatible with the initial purposes.

76 Council of Europe 108, art 5(b).

77 AU Convention, art 13, principle 3(a).

78 OECD Guidelines, par 9.

79 APEC Privacy Framework, par 22.

80 APEC Privacy Framework par 25 'uses of personal information'.

81 Bygrave (n 53) 173, 174; Roos (n 51)114.

82 Ibid.

This principle is stated simply in the OECD Guidelines,[83] the CoE Convention,[84] and the APEC Privacy Framework.[85] The GDPR and the AU Convention, however, add to the information quality principle in expressly requiring that reasonable steps be taken to ensure that personal data that is incomplete or inaccurate, in relation to the purposes for which they are processed, are erased or rectified.[86]

3.2.5 Data subject participation and control

Individuals should be able to participate in, and have a level of control over, the processing of their personal data by other individuals or entities.[87] Roos identifies six rights of data subjects that arise from this principle: (1) the right to have access to their personal data within a reasonable time and without excessive expense; (2) the right to request rectification, erasure or blocking of incomplete of inaccurate personal data, or data that has been processed in non-compliance with data protection principles or contrary to a legal provision; (3) the right to object to the processing of their personal data where such processing is justified to be necessary for the performance of a task carried out in the public interest or in the exercise of official authority, or for the legitimate interests of the controller of third parties to whom the data is disclosed; (4) the right to object to the processing of their personal data for direct marketing purposes, or to be notified beforehand of the disclosure of personal information to third parties for the purposes of direct marketing; (5) the right to object to the processing of data that will result in being subjected to automated decision making; and (6) remedies to enforce their rights to participate.[88]

As far as data subject participation is concerned, two notable rights afforded to data subjects surface in all of the relevant international instruments: (1) the right of access; and (2) the right of rectification or erasure. It can be deduced from the relevant international instruments that the right of access afforded to data subjects incorporates, firstly, the right to obtain from the data controller confirmation of whether or not personal data relating to him or her are held or being processed by

83 OECD Guidelines, par 8 'data quality principle'.
84 Council of Europe Convention 108, art 5(c) and (d).
85 APEC Privacy Framework par 27 'integrity of personal information'.
86 General Data Protection Regulation, art 5(1)(d); AU Convention art 13, principle 4.
87 Bygrave (n 53) 174-176.
88 For a thorough discussion of these principles, see Roos (n 51) 119-121.

the controller, and secondly, the right to have communicated to him or her the data relating to him or her.

According to the OECD Guidelines,[89] the GDPR,[90] the CoE Convention,[91] and the APEC Privacy Framework,[92] the appropriate personal data should be communicated to the data subject within a reasonable time, without excessive expense, in a reasonable manner, and in an intelligible form. The AU Convention similarly recognises the data subject's right to have communicated to him or her, the personal data undergoing processing, but contains no specifics on the form in which the or period by which the communication must be presented.[93]

As far as rectification rights are concerned, most data protection instruments have provisions which give persons the right to demand that incorrect, misleading or out-dated data relating to them be rectified or deleted by the data controller, and/or require that data controllers rectify or erase such data.[94] This is the case in the OECD Guidelines,[95] GDPR,[96] CoE Convention,[97] APEC Privacy Framework,[98] and the AU Convention.[99]

The GDPR further provides data subjects with the right to restrict processing of personal data,[100] the right to data portability,[101] the right to object to direct marketing or the processing of personal data in certain circumstances,[102] and rights related to automated decision making and profiling.[103]

3.2.6 Disclosure limitation

According to this principle, personal data should not be disclosed by the data controller to a third party, unless (1) the data subject consents to such disclosure; or

89 OECD Guidelines par 13(b).
90 General Data Protection Regulation, art 12(1), (3) and (5).
91 Council of Europe Convention 108, art 8(b).
92 APEC Privacy Framework, par 29(b).
93 AU Convention, art 17.
94, Bygrave (n 53) 176, 177.
95 OECD Guidelines, par 13(d).
96 General Data Protection Regulation, art 16 (right to rectification) and art 17 (right to erasure).
97 Council of Europe Convention 108, art 8(c) and (d).
98 APEC Privacy Framework, par 29(b).
99 AU Convention, art 19 (right of rectification or erasure).
100 General Data Protection Regulation, art 18.
101 Art 20.
102 Art 21.
103 Art 22.

(2) such disclosure is authorised by law.[104] This is mirrored in the OECD Guidelines as the 'Use Limitation Principle'.[105]

Roos describes the disclosure limitation principle as amounting to the application of the purpose specification principle to the disclosure of personal information. She indicates that the disclosure of data (which is a facet of the processing of data) would only be lawful or permitted if the disclosure is made in accordance with the specified, lawful purpose, or alternatively, where the data subject consents to the disclosure or where it is authorised by law. Roos' understanding aids this study in identifying elements of the disclosure limitation principle in international instruments where such principle is not explicitly mentioned.

The disclosure limitation principle can be found in the APEC Privacy Framework under the 'Uses of Personal Information' Principle, which stipulates in essence that the use of personal data collected should be limited to what is necessary to fulfil the purposes for which it was collected, except with the consent of the data subject;[106] when it is necessary to provide a service or product requested by the data subject;[107] or by the authority of law.[108] For the purposes of this APEC Privacy Principle, 'uses of personal information' includes the transfer or disclosure of personal information.[109] The disclosure limitation principle is not explicitly stated in the CoE Convention or the GDPR. Nor is it explicit in the AU Convention. However, the principle is implied by article 5(a) and (b) of the CoE Convention,[110] and can be construed from Principles 1 and 2 of Article 13 of the AU Convention.[111]

Both the GDPR and the AU Convention defines 'processing' to include the 'disclosure by transmission' of person data.[112] Elements of the disclosure limitation principle can be found in the GDPR under article 5(1)(a) and (b),[113] and article 6.[114]

---

104 Bygrave (n 53) 177.
105 OECD Guidelines, par 10.
106 APEC Privacy Framework par 25(a).
107 Par 25(b).
108 Par 25(c).
109 See the in-text commentary of par 25 in the APEC Privacy Framework.
110 Art 5(a) of the Council of Europe Convention 108 relates to the principle of fair and lawful processing; while art 5(b) concerns the purpose specification principle.
111 AU Convention, par 13, principle 1 (principle of consent and legitimacy of personal data processing) and principle 2 (principle of fair and lawful processing).
112 General Data Protection Regulation art 4(2) definition of 'processing'; AU Convention art 1 definition of 'processing of personal data'.
113 General Data Protection Regulation Art 5(1)(a) relating to the lawfulness, fairness and

Three notable circumstances arise in which the processing of personal data is deemed to be lawful: where the data subject consents to the processing of his or her data for specific purposes;[115] where processing is necessary for the performance of a contract that the data subject is party to or to take steps at the data subject's request;[116] and where the processing is authorised by law.[117]

3.2.7 Information security

The security principle requires data controllers to take reasonable security steps and safeguards to ensure that personal data is not accidentally destroyed or subject to unauthorised access, alteration, destruction or disclosure.[118]

This principle is embodied in the OECD Guidelines,[119] the GDPR,[120] the CoE Convention,[121] the AU Convention,[122] and the APEC Privacy Framework.[123] Unlike some of the other international instruments, the APEC Privacy Framework specifically states under the 'Security Safeguards' principle that such safeguards should be proportional to the probability and severity of the harm threatened, the sensitivity of the information and the context in which it should be held, and should be periodically reviewed and reassessed.[124] The GDPR provides a similar provision regarding the appropriate security measures to be taken by data controllers and processors, but takes into account additional considerations such as the state of the art, the costs of implementation and the nature, scope and purposes of the processing, amongst other aspects.[125]

---

transparency principle; and art 5(1)(b) relating to the purpose limitation or specification principle.

114 Art 6 relating to the lawfulness of processing.

115 Art 6(1)(a).

116 Art 6(1)(b).

117 Art 6(1)(c)- (e) read with art 6(3).

118 Bygrave (n 53) 177.

119 OECD Guidelines, par 11 'security safeguards principle'.

120 General Data Protection Regulation, art 5(1)(f).

121 Council of Europe Convention 108, art 7 'data security'.

122 AU Convention art 13, principle 6, and art 21 'security obligations' of the personal data controller.

123 APEC Privacy Framework, par 28.

124 Ibid.

125 General Data Protection Regulation, art 32 (1).

3.2.8 Data sensitivity

The principle of sensitivity requires that the processing of data which is considered especially sensitive for data subjects should be governed by stricter and more stringent controls than other personal data.[126]

OECD Guidelines does not differentiate between normal data and sensitive data.[127] Consequently, the OECD Guidelines do not prescribe additional safeguards for special categories of personal data.[128] Sensitive data may include, but is not limited to, data that relate to racial or ethnic origin, political opinions, religious or philosophical beliefs, or the health or sexual life of the data subject;[129] or data relating to criminal convictions.[130] The GDPR, the CoE Convention and the AU Convention all contain separate principles providing for the prohibition of the processing of sensitive data, including the aforementioned examples, and the exceptions to this prohibition.

The CoE Convention provides a general exception to the prohibition against the automatic processing of sensitive data, namely where domestic law provides appropriate safeguards.[131] The GDPR and the AU Convention provide particular circumstances where the processing or collection of sensitive data shall be permitted, which includes circumstances where the data subject has given explicit or written consent in conformity with existing law;[132] the processing relates to personal data which are manifestly made public by the data subject;[133]

While the APEC Privacy Framework does not provide data sensitivity as a separate information privacy principle, additional security safeguards for sensitive data is provided for under the Security Safeguards Principle, which stipulates that security safeguards should be proportional to the sensitivity of the information.[134]

---

126 Bygrave (n 53) 178.
127 Tan (n 46) 8, 9.
128 See Bygrave (n 53) at 178 for an explanation of why this principle is not included in the OECD Guidelines.
129 General Data Protection Regulation, art 9(1); Council of Europe Convention 108, art 6; AU Convention, art 14(1).
130 General Data Protection Regulation, art 10; Council of Europe Convention 108, art 6.
131 Council of Europe Convention 108 art 6
132 General Data Protection Regulation, art 9(2)(a); AU Convention art 14(2)(b).
133 General Data Protection Regulation, art 9(2)(e); AU Convention art 14(2)(a).
134 APEC Privacy Framework, par 28.

3.2.9 Openness or transparency

This principle requires that there be a general policy of openness about developments, practices and policies regarding personal data and the processing thereof.[135] Accordingly, data subjects should be made aware of the fact that their personal data are being processed, the purpose(s) for which this is done, the identity of recipients of their personal data, as well as the identity and usual residence of the data controller.[136]

This principle is expressed in the OECD Guidelines,[137] and is emphasised throughout the GDPR. Article 12 of the GDPR stipulates that data controllers must take appropriate measures to 'provide any information… and any communication… relating to the processing of personal data of the data subject in concise, transparent, intelligible and easily accessible form, using clear and plain language'.[138]

The AU Convention does not expand on the principle of openness, but simply states that principle of transparency requires 'mandatory disclosure of information on personal data by the data controller'.[139] The openness principle is also reflected in the data subject's right to information.[140]

The APEC Privacy Framework does not list the principle of openness or transparency as a separate privacy principle however the openness principle is embedded in the Notice principle.[141] The openness or transparency principle is not clearly set out in the CoE Convention, but can be implied from Article 8, which in essence, provides for information that the data subject is entitled to, such as the existence of an automated personal data file, its main purposes, as well as the identity and residence of the data controller.[142]

135 Roos (n 51) 116.
136 Idem at 117.
137 OECD Guidelines, par 12 'openness principle'.
138 General Data Protection Regulation, art 12(1).
139 AU Convention, art 13, principle 5 (principle of transparency).
140 Art 16.
141 APEC Privacy Framework, par 21-23 covering the Notice Principle.
142 Council of Europe Convention 108, art 8(a).

3.2.10 Accountability

The OECD Guidelines states under its 'Accountability Principle' that data controllers should be accountable for complying with measure which give effect to the above-stated principles.[143] The rationale is that it is the data controller who decides about and benefits from data processing activities, and consequently the controllers should be accountable under domestic law for complying with privacy protection rules and should not be released from this duty simply because another party is carrying out the data processing activities on their behalf.[144]

This principle is similarly set out in Article 5(2) of the GDPR, and paragraph 32 of the APEC Privacy Framework. The APEC Privacy Framework goes further in upholding the data controller's accountability for the protection of data even after the data has passed onto another organisation or jurisdiction.[145]

Accountability is not explicitly mentioned in the CoE Convention or the AU Convention, but can be implied from a holistic reading of the instruments.

3.3 Conclusion

The core principles of privacy and data protection discussed above can be found, in one form or another, in the OECD Guidelines, the APEC Privacy Framework, the GDPR, the CoE Convention and the AU Convention. It can be said that fair and lawful processing; minimality; purpose specification; information quality; data subject participation and control; disclosure limitation; information security; data sensitivity; openness and transparency; and accountability are all internationally agreed-upon principles that can establish a basic standard for privacy and data protection.

---

143 OECD Guidelines, par 14.

144 Original explanatory memorandum to the OECD Privacy Guidelines (1980) 32; Roos (n 51) 126.

145 Paragraph 32 of the APEC Privacy Framework adds that where 'personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with [the principles in the APEC Privacy Framework]'. For a further explanation of this paragraph, see the in-text commentary of paragraph 32 in the APEC Privacy Framework, and Tan (n 46) 20, 21.

CHAPTER 4 AN INTERNATIONAL COMPARISON OF THE APPROACHES TO PRIVACY AND DATA PROTECTION

4.1 Introduction

Different states take different approaches to data protection and online privacy. There are two main approaches to online privacy, namely the legislative approach and the self-regulation approach. These two positions will briefly be discussed in this chapter with reference to Europe and America. These approaches are particularly relevant for the purposes of the implementation of the core principles discussed in Chapter 3. Bearing these positions in mind, this chapter looks into the online privacy and data protection laws in the domestic legal frameworks of states across the globe. Reference will be made to the information on data protection laws of various states provided by DLA Piper, and presented in a table format in Appendix 1 of this study. This Chapter provides insight into global tendencies to realise online privacy and data protection rights, by reviewing the national privacy and data protection laws of various states.

4.2 The legislative approach and the self-regulation approach

The approaches to online privacy and data protection can generally be divided into two main categories: (1) the legislative approach; and (2) the self-regulation approach. Europe adopts a more restrictive position, namely the legislative approach, while the United States of America implements the self-regulation approach.

Europe regards the right to privacy as a fundamental human right, and consequently has more stringent laws protecting consumer privacy, which is effected by the government.[146] The United States of America, on the other hand, is more orientated on the non-interference by government, and thus the self-regulation approach is preferred to prevent the government from interfering in the affairs between private persons or entities.[147] Consequently, and there are no comprehensive laws on a

[146] Lindsay (n 1) 168, 169.

[147] Ibid; P O'Connor, 'An International Comparison of Approaches to Online Privacy Protection' (Information and Communication Technologies in Tourism, Vienna, 2005).

federal level in the United States that cover personal data protection in the private sphere.[148]

The European Union has assumed compulsory standards for consumer information through the GDPR, which encompasses the core principles of data protection discussed in the previous Chapter. The United States, on the other hand, has narrowly legislated mandatory standards for only certain types of consumer information, such as credit reporting data, health information, some types of financial transactions, and marketing data from minors.[149]

4.3 Online privacy protection in other domestic legal frameworks

As stated above, the OECD Guidelines and the APEC Privacy Framework are non-binding however they are still influential in the development of domestic data protection laws. Currently, there are thirty-five member states to the OECD. These member countries are: Australia, Austria, Belgium, Canada, Chile, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea, Latvia Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.[150] Over the past few decades, many member states of the OECD have enacted data protection legislation in their national legal frameworks. The twenty-one members of APEC are: Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong (China), Indonesia, Japan, Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, the Philippines, Russia, Singapore, Chinese Taipei, Thailand, the United States, and Vietnam.[151]

148 Lindsay (n 1) 168-169.

149 Z Tang, Y Hu and MD Smith, 'Gaining Trust through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor' (2008) 24(4) Journal of Management Information Systems 155.

150 OECD, 'List of OECD Member countries –Ratification of the Convention on the OECD' (OECD, 2018) <http://www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm> accessed 6 June 2018.

151 APEC, 'Member Economies' (APEC, 2017) <https://apec.org/About-Us/About-APEC/Member-Economies> accessed 6 June 2018.

As of 10 May 2018, only ten of the fifty-five AU member states have signed the AU Convention, and only two AU [152]member states have ratified the Convention. There are a number of data protection Bills awaiting enactment in the African region.

The study refers to the information provided by DLA Piper[153] on the domestic legislation in various countries around the world. The data protection laws of these countries have been presented in Table 1 in Appendix 1 of this study. From Table 1, it is evident that states, in general, are moving towards a legislative data protection framework. Various domestic data protection laws and/ or regulations have been enacted pursuant to the core principles of data protection discussed in the previous Chapter. Independent data protection authorities have been created and mandated by data protection legislation in many states. Alternatively, certain Ministerial departments are considered the competent data protection authority. One-hundred-and-nineteen independent data protection authorities from across the globe are members of a global forum called the International Conference of Data Protection and Privacy Commissioners (ICDPPC).[154] The ICDPPC provides leadership in data protection and privacy on an international level, and envisages 'an environment in which privacy and data protection authorities around the world are able effectively to fulfil their mandates, both individually and in concert, through diffusion of knowledge and supportive connections'.[155]

It appears that countries which do not yet have comprehensive or even general data protection laws still recognise the right to privacy both offline and online. Many countries that do not have general data protection laws criminalise conduct that infringes the right to privacy online. Where there is no competent data protection authority, the courts are usually the appropriate authority to hear and grant remedy for the infringement of privacy in the online context, or for the violation of data protection rights.

---

152 AU, 'List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection' obtained from <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed on 6 June 2018. The member states who have signed the Convention are Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe, and Zambia. Only Mauritius and Senegal have ratified and deposited the Convention into their domestic law.

153 DLA Piper (n 31).

154 International Conference of Data Protection and Privacy Commissioners (ICDPPC), 'Home Page' obtained from <https://icdppc.org> accessed on 3 June 2018.

155 ICDPPC, 'Mission and Vision' obtained from <https://icdppc.org/the-conference-and-executive-committee/strategic-direction-mission-and-vision/> accessed on 3 June 2018.

A few states have enacted legislation that cover online privacy issues specifically, such as the use of third-party cookies, traffic data and location based services. The application of these provisions, however, is often limited to electronic communication service providers and electronic network service providers. However, more often than not, the general data protection principles of that state will apply to online privacy issues. The study will now investigate whether the standard of data privacy protection outlined in Chapter 3 has formed a rule of general international law in customary international law.

CHAPTER 5 THE CORE PRINCIPLES OF DATA PROTECTION AS CUSTOMARY INTERNATIONAL LAW

5.1 Introduction

As a point of departure, the right to privacy is a fundamental right and can be regarded as a customary international rule. Using a modern approach, Zalnieriute concludes that data privacy has indeed developed into a separate rule of customary international law.[156] While these rights have formed customary international laws in themselves, the standards of data privacy protection to be adopted are not as clear. This chapter seeks to determine whether a standard for data protection has formed a customary international law, and can subsequently be enforced.

The traditional approach to customary international law is found in Article 38(1)(b) of the Statute of the International Court of Justice (ICJ).[157] This provision provides for the two elements required for the establishment or formation of a customary international law, namely (1) state practice; and (2) *opinio juris*.[158]

5.2 State practice

Evidence of state practice can be deduced from the conduct of a state. Evidence of general state practice can be found in treaties, decisions of both national and international courts, national legislation, International Law Commission reports and the comments thereon by states, and resolutions of the political organs of the United Nations.[159] This list is not exhaustive. A state's silent acquiescence in or tolerance of a rule, or its failure to protest against an emerging rule, can also constitute evidence of state practice.[160] While universal acceptance is not necessary,[161] there must be 'general' or 'widespread' acceptance for a rule to qualify as an international custom.[162]

---

156 M Zalnieriute, 'An international constitutional moment for data privacy in the times of mass-surveillance' (2015) International Journal of Law and Information Technology 1-35.

157 Statue of the International Court of Justice of 1945, art 38(1)(b).

158 Article 38(1)(b) provides that an international custom may form where there is 'evidence of a general practice accepted as law'.

159 J Dugard, *International Law: A South African Perspective* (4th edn, Juta 2011) 26.

160 Ibid.

161 *North Sea Continental Shelf Cases* 1969 ICJ Reports 3 at 229.

162 *Fisheries Jurisdiction case* 1974 ICJ Reports 3 at 23-6.

According to the Paper presented at Expert Workshop on the Right to Privacy in the Digital Age, in February 2018,[163] out of the 193 member states of the UN, over 70 states have no privacy law at all.[164] Out of the remaining UN member states, less than half have certain key essential characteristics like a truly independent data protection authority or truly stringent enforceable safeguards and remedies.[165]

While this may not seem impressive, continuous efforts have been made by states to adopt and improve privacy and data protection laws. Greenleaf declares that between 2015 and 2017, the number of states that had enacted data privacy laws rose from 109 to 120.[166] He adds that these 120 states 'have comprehensive data privacy laws for the private sector, public sector, or (in most cases) both, and the laws meet at least minimum formal standards based on international agreements'.[167] These 120 states, categorised by Greenleaf according to geographic region, comprises of 28 states belonging to the EU; 26 other European states; 21 African states; 13 states from Asia; 10 states from the Caribbean; 10 Latin American states; 6 states from the Middle East; 2 North American states; 2 Australasian states; and 2 states from Central Asia.[168] Greenleaf notes that the Pacific Island region is the only region without any official or draft legislation with regard to data privacy.[169] Greenleaf notes in 2017, that 'the increase [of] countries with data privacy laws…, … the additional countries planning to enact such laws, and the bills to strengthen existing laws, all underline the continuing global expansion of data privacy laws'.[170]

The principles of the United Nations' Guidelines for the Regulation of Computerized Personal Data Files[171] are similar to those core principles discussed in Chapter 3. These principles, along with the privacy principles contained in the OECD Guidelines

163 UN Human Rights Council 'Report of the Special Rapporteur on the Right to Privacy' (2018) UN Doc A/HRC/37/62 (advance unedited version), Annex: Paper presented at expert workshop on the right to privacy in the digital age, Office of the High Commissioner for Human Rights.

164 Idem at 28, par 18 and 19 of the Annex.

165 Idem at 28, par 20 of the Annex.

166 G Greenleaf, 'Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey' (2017) 145 Privacy Laws & Business International Report 10-13.

167 Ibid. The 'minimum formal standards based on international agreements' that Greenleaf refers to is the OECD Guidelines and the CoE Convention Guidelines.

168 Ibid.

169 Ibid.

170 Ibid.

171 'Guidelines for the Regulation of Computerized Personal Data Files' adopted by UN General Assembly Resolution A/RES/45/95 (14 December 1990) UN Doc E/CN.4/1990/72.

and the CoE Convention, have informed data privacy laws across the globe.[172] Though the UN privacy and data protection principles are non-binding, they are influential.

Many states have signed international or regional treaties or conventions which endeavour to, amongst other things, advance free flow of information while protecting fundamental values of privacy and individual liberties. Many states have enacted or improved existing data protection legislation pursuant to privacy guidelines.[173] All member states of the Council of Europe have ratified the CoE Convention.[174] The GDPR and its privacy and data protection principles are binding upon all members of the EU, irrespective of whether or not the member States of the EU have implemented the GDPR through domestic legislation. Nonetheless, EU member States have already enacted GDPR implementing legislation, and have supplemented the GDPR with new or amended data protection laws.[175] Other EU members, such as Bulgaria, Czech Republic, Estonia, Finland, Greece, Portugal, Slovenia, Spain, have drafted implementing legislation but are yet to enact it.[176] Furthermore, non-EU member States, such as Guernsey,[177] Iceland,[178] and Norway,[179] have also adapted their law to comply with the GDPR, while other States, such as India,[180] Serbia,[181] Switzerland,[182] and Thailand,[183] are still in the process of

172 Greenleaf (n 165) 10-13.
173 Ibid.
174 Council of Europe, 'Chart of signatures and ratifications of Treaty 108' (Council of Europe, 27 June 2018) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=XOI51XuE> accessed 27 June 2018.
175 These States include Austria, Belgium, Croatia, Cyprus, Denmark, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Romania, Slovakia, Sweden, and the United Kingdom. Baker McKenzie, 'GDPR National Legislation Survey, 4.0' (*Baker McKenzie*, August 2018).
176 Baker McKenzie (n 175).
177 DLA Piper (n 31) 218.
178 Persónu Vernd, 'General Introduction' (*Persónu Vernd*, 2018) <https://www.personuvernd.is/information-in-english/greinar/nr/437> accessed on 14 October 2018.
179 AS Wiersholm, 'Data Protected – Norway' (*Linklaters*, September 2018) <https://www.linklaters.com/en/insights/data-protected/data-protected---norway> accessed 4 October 2018.
180 A Regidi, 'Data Protection Bill Series: Quick Overview of India's Draft Data Protection Law' (*Tech2*, 28 July 2018) <https://www.firstpost.com/tech/news-analysis/data-protection-bill-series-quick-overview-of-indias-draft-data-protection-law-4841321.html> accessed 14 October 2018.
181 DLA Piper (n 31) 504.
182 Idem at 570.
183 H Boonklomjit, N Rerknithi, A Gamvros and R Kwok, 'Overview of Thailand Draft Personal

doing so. It is clear that both member and non-member States of the EU have revised their data privacy law to comply with the GDPR. In doing so, these States would have incorporated all the basic data protection principles outlined in Chapter 3.

The OECD Guidelines are regarded as a remarkable success.[184] The OECD Guidelines are considered to represent an international consensus on personal data handing protection in both the public and private sectors.[185] The OECD Guidelines have greatly influenced the drafting of domestic data protection legislation globally, and many states have based their legislated information privacy principles directly on the Guidelines.[186] States have furthermore expanded on the Guidelines and have added additional protection. Examples include the Australian Privacy Act of 1988, as amended in 2001;[187] New Zealand's Privacy Act of 1993, as amended in 2010;[188] the Personal Information Protection and Electronic Documents Act (PIPEDA) of 2001 of Canada;[189] Japan's Act on the Protection of Personal Information of 2003;[190] Korea's Act on the Promotion of Information and Communications Network Utilization and Data Protection Act of 2001, as amended;[191] Mexico's data protection legislation;[192] and the Constitution of Turkey as amended in 2010.[193]

Data Protection Act' (Norton Rose Fulbright, 6 August 2018) <https://www.dataprotectionreport.com/2018/08/overview-of-thailand-draft-personal-data-protection-act/> accessed 20 October 2018.

184 OECD, *The OECD Privacy Framework* (OECD Publishing 2013) Chapter 4 The evolving privacy landscape: 30 years after the OECD Privacy Guidelines (2011), 65.

185 Ibid.

186 Idem at 77.

187 Ibid. The eleven Information Privacy Principles contained in the Australian Privacy Act of 1988 are directly built on the OECD Guidelines. The amendment to the Act extended the application of the Act to cover the private sector, and added ten National Privacy Protection which include principles covering transborder data flows, anonymity and identifiers.

188 Ibid. The New Zealand Privacy Act elaborates on the OECD's Collection Limitation and Purpose Specification Principles, and further includes principles on unique identifiers. The 2010 amendment explicitly refers to the OECD Guidelines, indicating the continuing influence of the Guidelines.

189 Ibid. PIPEDA applies only to the private sector, and is modelled on the OECD Guidelines. The Act offers additional protection.

190 Idem at 77 and 78. This Act applies to certain private businesses. Furthermore, various ministries of Japan develop sector-specific guidelines.

191 Idem at 78. The Act generally applied the OECD Guidelines, but initially applied only to providers of information and communications networks. The Act was later broadened to include additional types of businesses, and required the government to develop policies that promote the use of security measures and protect personal data.

192 Ibid. The *Ley Federal de Protección de Datos Personales en Posesión de los Particulares 2010* of Mexico incorporates the OECD Guidelines.

193 Ibid. Turkey's Constitution was amended to afford individuals additional rights relating to the

Sector-specific legislation in areas such as health, financial information and telecommunications has been adopted in many countries. These sector-specific legislations often contain provisions that protect the privacy of information in those specific industries. Components of the OECD Guidelines can be found in legislation other than legislation particularly dedicated to data protection law.[194] The OECD Guidelines are also useful for states that adopt a self-regulatory approach with regards to privacy and data protection. The Guidelines have provided the foundation for multiple privacy policies in the private sector, self-regulatory policies and model codes.[195]

APEC recently developed the Cross-Border Privacy Rules (CBPR) system in terms of which companies trading within the member economies cultivate their own internal business rules consistent with the APEC Privacy Principles to secure cross-border data privacy.[196] The APEC CBRP system was endorsed by the APEC member economies in 2011.[197] As of September 2017, five APEC economies partake in the CBPR system, namely Canada, Japan, Mexico, South Korea and the United States of America. Organisations that elect to partake in the CBPR system are required to submit their privacy policies and practices for evaluation by an accountability agent recognised by APEC to appraise compliance with the CBPR system requirements, including the APEC Privacy Framework.[198] Once certified, the policies and practices become binding on that organisation and will be enforceable by the relevant privacy enforcement authority.[199]

Some APEC member states, such as China, the Philippines, Thailand and Peru, appear to lean more towards a European Union approach to privacy protection than the APEC Privacy Framework with regard to the drafting of domestic legislation and their Bills.

---

protection of their personal data, and to address matters of consent, use limitation, access and correction.

194 OECD, *The OECD Privacy Framework* (n 174) 79.

195 Ibid.

196 ER Cooper and AC Raul (n 47) 27, 31. It must be noted that the APEC CBPR system is a voluntary accountability-based system that governs the electronic trans-border flows of private data among APEC economies.

197 Idem at 31.

198 Ibid.

199 Ibid.

DLA Piper reveals in its Handbook that most of the national data protection laws of the states referred to in the Appendix of this study contain the basic principles of data and privacy protection.[200] Component of the basic principles of data privacy protection can also be found in sector-specific national laws of states. Various countries that fall short of the standard of data privacy protection endeavour to incorporate the core privacy and data protection principles through the enactment or amendment data protection legislation, or through regulations.[201]

Some of the basic principles of data privacy protection are also reflected in the common law accepted by states. An example of this can be found in the legal framework of the British Virgin Islands. British Virgin Islands has no data protection legislation. However the government of the British Virgin Islands has undertaken to enact data protection legislation centred on internationally recognised standards, in the near future. Despite the absence of legislation, entities that manage and maintain personal information data are required to observe English common law duties of confidentiality and privacy.[202] The common law duty of confidentiality entails that personal information shall be confidential, and may not be misused or be disclosed without proper authorisation.[203] This common law duty is applicable in cases concerning the collection and processing of personal data, the transfer of personal data to a third party, and the security of personal data.[204] The common law duty of confidentiality similarly finds application in Bermuda and the Cayman Islands.[205]

It appears that more states are moving towards a comprehensive legislative approach to online privacy, and are enacting or amending data privacy laws. Though there are still states that are adamant on maintaining a self-regulatory framework, acceptance of core data and privacy protection principles can still be found in means other than the adoption of law. The EU-U.S. Privacy Shield Framework that was designed by the United States Department of Commerce and European Commission serves as evidence of the United States' acceptance of the basic privacy and data protection principles.[206] The EU-U.S. Privacy Shield contains Privacy Principles,

200 DLA Piper (n 31).
201 Ibid.
202 Idem at 70-71.
203 Idem at 63, 71, 90.
204 Idem at 70-71.
205 Idem at 63, 91.
206 United States of America Department of Commerce, 'EU-U.S. Privacy Shield' (Department of

consistent with those core principles above, which companies must observe in order to receive and use personal data from the EU.[207]

5.3 Opinio juris

For the second element to be present, state practice must be 'accepted as law'.[208] This is known as *opinio juris* and entails a psychological element, on the part of states, to be bound by a particular rule.[209] It is difficult to produce evidence of *opinio juris*.[210] There are no clear guidelines on how *opinio juris* can be determined. *Opinio juris* becomes more difficult to identify in a self-regulatory legal framework.

Considering the emphasis of privacy and data protection by international bodies or organisations, the international pressure on states to provide comprehensive privacy and data protection laws, and the subsequent enactment or amendment of data privacy legislation by states, it can be said that states recognise the importance of online privacy and data protection in the digital age. States are encouraged to accept and integrate the core privacy and data protection principles, as set out in various international instruments discussed in Chapter 3, into their local law. Many states have conformed to this though their reasoning for doing so may differ. For instance, Europe protects the right to privacy as a fundamental and basic human right, while Asia-Pacific regions are often economically motivated and privacy protection as being necessary to ensure global commerce and free flow of information.

5.4 Conclusion

The fundamental right to privacy has become a rule of customary international law. This right extends to privacy in the online environment. It appears that the acceptance and use of the core privacy principles discussed in Chapter 3 has become state practice. This is evident from the on-going efforts that states have made to enact and improve data protection laws to give effect to and enforce the right to online privacy. While the application and interpretation of the core data and

---

207 Commerce) <https://www.commerce.gov/tags/eu-us-privacy-shield> accessed 10 June 2018. See European Commission, 'Guide to the EU-U.S. Privacy Shield' (European Commission, 2016) available on <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en> accessed 10 June 2018.

208 ICJ Statute, art 38(1)(b).

209 Dugard (n 159) 29-30.

210 Ibid.

privacy protection principles are not necessarily uniform, they are contained in some form in the domestic legal frameworks of many states. Many states have officially incorporated the basic privacy principles through legislative means. States have approved and validated privacy principles and guidelines that have been laid down in the various regional instruments. Regardless of which regional privacy principles have been endorsed and/ or incorporated into domestic law by states –be it the OECD Guidelines, the APEC Privacy Framework, the CoE Convention, the EU Directive, the GDPR, or even the AU privacy and data protection principles –what these states all have in common is the acceptance of the underlying core principles of privacy and data protection. Further evidence of state practice can be found in agreements established between states, such as the EU-U.S. Privacy Shield, which require the basic principles of privacy and data protection to be observed where trans-border flows of personal data is concerned.

States have recognised the importance of privacy over the internet, and have consequently accepted the basic privacy principles as law. All these factors indicate an international consensus of the acceptance and applicability of the basic privacy and data protection principles. It can therefore be said that the core privacy and data protection principles outlined above constitute a rule of customary international law. Thus the core privacy and data protection principles should be treated as the basic standard of privacy protection in general international law which can be applied universally.

CHAPTER 6 EFFECTIVE IMPLEMENTATION OF INTERNATIONAL STANDARDS

6.1 Introduction

Given the magnitude of trans-border flows of data that occur daily and the problem of jurisdiction over cyberspace and other interests, it is especially necessary to regulate the internet. Enforcement of online privacy may require one to look beyond the traditional division between states and private entities in international law as the internet goes beyond territorial jurisdiction.

6.2 'Trust mark'

O'Connor discusses a possible means of implementing an international standard globally, namely the 'trust mark'.[211] This entails that an independent third party will certify a company if the company meets certain prescribed standards. Trust marks rely on consumers' trust. In terms of this model, certifying organisations encourage companies to behave ethically by providing specific guidelines to protect and assure minimal standards; compelling companies to undergo a review to establish compliance with these standards; requiring companies to submit to periodic re-verification and to commit to a resolution procedure in case of dispute.[212]
However, this approach faces many challenges in practice. There is a lack of enforcement when companies violate the terms of their marks. Trust marks can only succeed if they remain credible in the mind of the consumer.[213]

6.3 International environmental law model

Authors submit that a new international law model should be devised with respect to the governance of the internet and cyberspace, so as to cater for the growing and dynamic legal and technological field.

The model of international environmental law may be an appropriate model to regulate internet law and cyber law. The international environmental law model is

211 O'Connor (n 147).
212 Ibid.
213 Ibid.

premised on international cooperation.[214] Threats to the environment demand a concerted, co-operative effort which employs existing customary international law rules and the treaty as a legislative instrument, whilst also engaging new methods for securing international co-operation.[215] Thus the international environmental model was formed. This model is a blend of 'hard law' –that is customary international rules and treaties– and 'soft law' –which comprises of conference resolutions, guidelines and programmes of action.[216] 'Soft law' plays a fundamental role in environmental law.[217] This is primarily due to the lengthy procedures required to form treaties and customary international rules, and the difficulty in acquiring the consent of states to treaties relating to environmental issues in urgent cases.[218] Soft law is therefore preferred to bypass the difficulties that hard law poses. It is usually soft law that forms the guidelines which the states then adopt.

Important in this model is state responsibility. States have an obligation not to use or allow its territory to be used in a way that causes harm or injury to the territory of another state or to persons or property of that state.[219] This entails that states are responsible for private persons within its territory.[220] This model is also founded on international co-operation. All states act in a common interest and focuses on prevention and regulation rather than reparation and adjudication. [221]

A similar model could be developed for internet law and cyber law. Should this model be applied to the internet law and cyber law framework, states would be required to enforce a certain prescribed set of international standards that would be indirectly binding upon companies. States would be responsible for the conduct of private entities within its territory, thus states would have to ensure that companies comply with international standards too.

214 Dugard (n 159) 400.
215 Ibid.
216 Ibid.
217 Idem at 401.
218 Idem at 34.
219 Idem at 402-403.
220 Ibid.
221 Idem at 405.

7 CONCLUSION

The right to privacy is a fundamental human right that deserves legal protection by all nations. This right has been recognised on an international and national level. The Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and other international instruments emphasise the protection of fundamental human rights, which include the right to dignity and the right to privacy. Furthermore, the right to privacy is recognised as a fundamental human right in the Constitutions of most states. The right to privacy extends to privacy in the online environment. Online privacy is of public interest and has gained much attention with the rise of the digital era. The lack of regulation and the problems relating to jurisdiction over the internet opens doors for possible abuse and infringement on human rights amongst other things. With the growth of the use of the internet, there has been a need to devise a coherent and uniform standard of privacy protection that can apply universally and can be enforced.

Privacy is a broad concept which includes aspects such as informational privacy and privacy of communications. Privacy in the online environment has given rise to the concept of data protection. While data protection and privacy are two distinct and separate concepts, they can overlap and inform each other. Data protection can be seen as a mechanism to actualise the right to privacy. In other words, individuals can enjoy their right to privacy where they are able to control the use and/or collection of their personal data by other parties, or are at least made aware of such use or collection and the purposes for which their personal data is being used or collected.

Many states have devised and enacted legislation and regulations that particularly address data protection. However not all state have made provision in their legal frameworks for specific online privacy issues such as cookies, location data and traffic data. In countries that do not specifically address these aspects, general data protection law may become applicable. Thus it is important to establish what the general data protection law consists of, in particular, what the basic standard of privacy protection to be applied is or should be. Various international and regional bodies and organisations have sought to answer this question.

The United Nations, the European Union, the African Union, the Organisation for Economic Co-operation and Development, the Asia-Pacific Economic Co-operation, and the Council of Europe have each constructed their own set of data and privacy protection principles. Though these principles may be structured differently or are based upon a particular background, common and core ideas run through them and can be identified as the principles of fair and lawful processing; minimality; purpose specification; information quality; data subject participation and control; disclosure limitation; information security; data sensitivity; openness and transparency; and accountability.

Having established a similar set of principles from the various regional bodies, the question then posed is whether these principles constitute a rule of customary international law. For a norm or standard to constitute a rule of customary international law, two requirements must be met. The first requirement is that there must be state practice, and the second is that the state practice must be accepted as law (*opinio juris*).

Various states are members of regional bodies which aim to address privacy and data protection on an international and national level. As mentioned above, these bodies have provided their own set of privacy protection guidelines, which have been endorsed by the member states of these bodies. The OECD Guidelines, which contain the core privacy principles, has been particularly influential in the formation of domestic data protection laws, legislation and regulations of numerous countries. The core privacy principles have been incorporated into the domestic legal frameworks of many states across the globe. States have expressly and implicitly accepted the applicability of the core data privacy principles through bilateral or multilateral agreements, in which the contracting state is required to observe basic privacy principles where trans-border flows of personal data is concerned. States continue to create new data and privacy protection laws or regulations, or to develop and improve existing laws that comply with the core data privacy principles. It has become state practice to accept and apply the core principles of data and privacy protection.

States recognise the importance of protecting and giving effect to the fundamental right to privacy, especially in the growing digital age. States have accepted the core

principles as law, to which they have bound themselves through domestic law or through international agreements concerning trans-border flows of personal data. Thus this study concludes that the core data and privacy principles –namely the principles of fair and lawful processing; minimality; purpose specification; information quality; data subject participation and control; disclosure limitation; information security; data sensitivity; openness and transparency; and accountability –has become a rule of customary international law. The core privacy principles, as a rule of general international law, should thus be applicable universally.

Given the unique nature of the internet and the problem of jurisdiction over activity on the globally connected network, enforceability of the core privacy principles becomes a problem. The internet is not limited by geographic jurisdiction and the question that arises is what body would have the authority to enforce data and privacy protection principles where trans-border flows of personal data is concerned.

This study proposes that a new international law model, similar to the international environmental law model, be developed for internet and cyber law. Such a model would be a hybrid system of both ‘hard’ law and ‘soft’ law, which would be regarded as equally binding by states, and would be based on state responsibility and international co-operation. This dynamic model would allow international law to keep up with technological and cyber advancements.

The right to privacy has undergone much development over the years.

8 APPENDIX 1 – TABLE 1: INTERNATIONAL COMPARISON OF DATA PROTECTION AND ONLINE PRIVACY LAWS[222]

COUNTRY	IS THERE LEGISLATION THAT IS SPECIFICALLY DEDICATED TO DATA PROTECTION?	ARE THERE SPECIFIC LAWS THAT PROVIDE FOR ONLINE PRIVACY PROTECTION?[223]	IS THERE A SPECIFIC ENFORCEMENT BODY FOR DATA PROTECTION?
Angola[224]	• Law No. 22/11 on the Protection Law of Personal Data of 17 June • Law No. 7/17 on the Protection of Information Systems and Networks of 16 February	Law No. 23/11 on Electronic Communications and Information Society Services of 20 June	Not yet created
Argentina[225]	Personal Data Protection Law No. 25,326 of October 2000	None	Yes
Australia[226]	• The Federal Privacy Act 1988 (Cth) and its Australian Privacy Principles • Information Privacy Act 2014	• Federal Privacy Act • State and Territory privacy laws	Yes
Austria[227]	Data Protection Act, as amended	Telecommunications Act 70/2003	Yes
Bahrain[228]	Sector-specific legislation	None	Information and e-Government Authority available
Belarus[229]	Law on Information, Informatisation and Information Protection of 10 November 2008 No. 455 Z	General requirements for personal data protection are applicable	Yes (not independent from

222 The information contained in this table was obtained predominantly from DLA Piper (n 31).
223 Note that "online privacy protection" here particularly refers to protection of location and traffic data, and the use of cookies and similar technologies.
224 DLA Piper (n 31) 8-13.
225 Idem at 14-18.
226 Idem at 19-24.
227 Idem at 25-34; Republik Österreich Datenschutzbehörde, 'Data protection law in Austria' (*Republik Österreich Datenschutzbehörde*, 2018) <https://www.dsb.gv.at/gesetze-in-osterreich> accessed 1 October 2018.
228 DLA Piper (n 31) 35-39.
229 Idem at 40-43.

			government)
Belgium[230]	Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data	Act of 13 June 2005 on Electronic Communications	Yes
Bermuda[231]	Personal Information Protection Act 2016 (not yet fully operational)	None	Yet to be appointed
Bosnia and Herzegovina[232]	The Law on Protection of Personal Data, as amended	General data protection rules apply	Yes
British Virgin Islands[233]	None	None	None
Bulgaria[234]	GDPR	• Electronic Communications Act is applicable where traffic and location data is retained/ processed by electronic communications service providers (ECSPs) • General regime for processing of personal data applies	Yes
Canada[235]	Canadian Privacy Statutes: • Personal Information Protection and Electronic Documents Act (PIPEDA) • Personal Information Protection Act (PIPA Alberta) • Personal Information Protection Act (PIPA BC) • Act Respecting the Protection of Personal Information in the Private Sector (Quebec Privacy Act)	Canadian Privacy Statutes	Multiple authorities exist and are mandated by the various Acts in place
Cape Verde[236]	Data Protection Law (Law No. 133/V/2001 of 22 January 2001, as amended by Law No. 41/VIII/2013)	Law No. 134/V/2001 provides for protection of personal data and traffic data in the telecommunications sector	Yes

230 Idem at 44-54; Baker McKenzie (n 175) 2.
231 DLA Piper (n 31) 55-57.
232 Idem at 58-62.
233 Idem at 63-65.
234 Idem at 66-79.
235 Idem at 80-86.
236 Idem at 87-90.

Cayman Islands[237]	Data Protection Law, 2017 (not yet in force)	None	None
China (Peoples' Republic of China)[238]	• Cybersecurity Law 2017 • The Decision on Strengthening Online Information Protection 2012 • National Standard of Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services 2013 • Sector-specific legislation	• The Decision on Strengthening Online Information Protection • Consumer Protection Law 2014 • Cybersecurity Law 2017 Online privacy for mobile apps: • Administrative Provisions on Administration of Information Services of Mobile Internet Application Programs	Sector-specific regulators
Costa Rica[239]	Law No. 8968, Protection in the Handling of the Personal Data of Individuals, and its by-laws	General rules of data protection issued by the Constitutional Court	Yes
Croatia[240]	Law on the Implementation of the General Data Protection Regulation, 2018	• Electronic Communications Act • All data protections rules are applicable	Yes
Cyprus[241]	Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of Such Data of 2018	Part 14 of the Electronic Communications and Postal Services Law (applicable to publically available ECSPs)	Yes
Czech Republic[242]	GDPR	Act No. 127/2005 Coll. on Electronic Communications	Yes
Denmark[243]	Data Protection Act 2018	• Act on Electronic Communications Services and Networks 2011 • Executive Order on Information and Consent Required in Case of Storing and Accessing Information in End-user Terminal Equipment 2011	Yes
Egypt[244]	No specific general data protection legislation.	None	None

237 Idem at 91-93.
238 Idem at 94-101.
239 Idem at 102-104.
240 Idem at 105-114.
241 Idem at 115-127; Baker McKenzie (n 175) 4.
242 DLA Piper (n 31) 128-137.
243 Idem at 138-145.

	• The Constitution and the Egyptian Civil Code regulate the collection and processing of personal data • Sector-specific legislation		
Estonia[245]	GDPR	Collection/ retention of traffic and location data only covers telecommunications industry (Consent to cookies not required due to the opt-out system)	Yes
Finland[246]	• GDPR • Sector-specific legislation	Law on Electronic Communications 917/2004	Yes
France[247]	Law No. 2018-493 of 20 June 2018 on the Protection of Personal Data	• EU Cookie Directive and the updated recommendations for cookies issued by the French data protection authority • Postal and Electronic Communications Code applicable to telecommunications service providers	Yes
Germany[248]	Federal Data Protection Act of 30 June 2017. Each German state has its own data protection law.	Federal Data Protection Act applicable	Yes
Ghana[249]	Data Protection Act 843 of 2012	None	Yes
Gibraltar[250]	Data Protection Act 2004	The Communications (PD&P) Regulations 2006 (applicable to ECSPs)	Yes
Greece[251]	GDPR	Articles 4 and 6 of Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data, as amended by Directive 2009/136/EC (applicable to ECSPs)	Yes

244 Idem at 146-148.
245 Idem at 149-161.
246 Idem at 162-176.
247 Idem at 177-187.
248 Idem at 188-198.
249 Idem at 199-202.
250 Idem at 203-207.
251 Idem at 208-217.

Guernsey[252]	• Data Protection Law, 2017 • Data Protection (Commencement, Amendment and Transitional) Ordinance, 2018 • Data Protection (Law Enforcement and Related Matters) Ordinance, 2018	European Communities (Implementation of Privacy) Directive (Guernsey) Ordinance 2004	Yes
Honduras[253]	No general data protection legislation • Constitution of the Republic of Honduras, 1982 (Article 182) • Law of the Civil Registry (Article 109) • Law for Transparency and for Access to Public Information (Article 3.5) • Rulings on the Law for Transparency and for Access to Public Information (Article 42)	None	Yes
Hong Kong[254]	Personal Data (Privacy) Ordinance, as amended	Personal Data Ordinance applicable	Yes
Hungary[255]	Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information, as amended by Act XXXVIII of 2018 and Act XIII of 2018	Act C of 2003 on Electronic Communications applies to collection of location and traffic data by public ECSPs and the use of cookies	Yes
Iceland[256]	Act No. 90/2018 on Data Protection and the Processing of Personal Data	Provisions of Data Protection Act are applicable	Yes
India[257]	Sector-specific legislation	None	None
Indonesia[258]	Regulations on the use of electronic data: • Law No. 11 of 2008 Concerning Electronic Information and Transactions, as amended • Government Regulation No. 82 of 2012 regarding Provisions of Electronic systems and Transactions	None	No

252 Idem at 218-223.
253 Idem at 224-227.
254 Idem at 228-232.
255 DLA Piper (n 31) 233-242; Baker McKenzie (n 175) 7.
256 DLA Piper (n 31) 243-252; Persónu Vernd (n 178).
257 DLA Piper (n 31) 253-257; A Regidi (n 180).
258 DLA Piper (n 31) 258-264.

	• Minister of Communications and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System • Sector-specific regulations		
Ireland[259]	Data Protection Act 2018	• European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 • Office of the Data Protection Commissioner's regulatory guidance on the use of cookies	Yes
Israel[260]	No general data protection law • Protection of Privacy Law, 5741-1981 as amended 1996, and the regulations promulgated thereunder • Guidelines of the Israel Privacy Authority	General principles of Protection of Privacy Law apply	Yes
Italy[261]	Legislative Decree No. 101/2018	'Privacy Code' (Legislative Decree No. 196/2003), as amended	Yes
Japan[262]	Act on the Protection of Personal Information, as amended	None	Yes
Jersey[263]	Data Protection Law 2018	General principles of the Data Protection Law apply	Yes
Latvia[264]	Personal Data Processing Law, 2018	• Law on Electronic Communications • Law on Information Society Services	Yes
Lesotho[265]	Data Protection Act 2013	None (however future regulations may be issued	Yes

259 Idem at 265-277; Baker McKenzie (n 175) 9.

260 DLA Piper (n 31) 278-282.

261 Idem at 283-293; Gianni, Origoni, Grippo, Cappelli & Partners (October 2018) 'Data Protected – Italy) <https://www.linklaters.com/en/insights/data-protected/data-protected---italy> accessed 4 October 2018.

262 DLA Piper (n 31) 294-299; Personal Information Protection Commission Japan 'Laws and Policies' (*Personal Information Protection Commission, Japan*, 2018) <https://www.ppc.go.jp/en/legal/> accessed 16 October 2018.

263 DLA Piper (n 31) 300-303.

264 Idem at 304-315; Ministry of Justice of the Republic of Latvia, 'Latvia is the first among the Baltic States to adopt the Personal Data Processing Law' (*Ministry of Justice of the Republic of Latvia*, 21 June 2018) <https://www.tm.gov.lv/en/news/latvia-is-the-first-among-the-baltic-states-to-adopt-the-personal-data-processing-law> accessed on 14 October 2018.

265 DLA Piper (n 31) 316-320.

		under the Act to address online privacy matters)	
Lithuania[266]	Law on Legal Protection of Personal Data, amended on 16 July 2018	Law on Legal Protection of Personal Data	Yes
Luxembourg[267]	Law of 1 August 2018 on the Organization of the National Commission for Data Protection and the General Rules on Data Protection	Data Protection Law	Yes
Macau[268]	Law No. 8/2005 on the Protection of Personal Data	General data protection rules contained in Law No.8/2005 apply	Yes
Macedonia[269]	The Law on Personal Data Protection	General data protection rules contained in the Law on Personal Data Protection apply	Yes
Madagascar[270]	Law No. 2014-038 relating to protection of personal data	None	Not yet established
Malaysia[271]	Personal Data Protection Act 2010	None (however Data Protection Commissioner may issue guidance in future on online privacy matters)	Yes
Malta[272]	Data Protection Act, 2018	Processing of Personal Data (Electronic Communications Sector) Regulations, as amended (applicable to telecommunications service providers)	Yes
Mauritius[273]	Data Protection Act 2017	Data Protection Act applicable	Yes
Mexico[274]	• Federal Law on the Protection of Personal Data held by Private Parties 2010 • The Regulations to the Federal Law on the	• 'Regulations' • 'Guidelines'	Yes

266 Idem at 321-333; Teisės Aktų Registras, 'Law on Legal Protection of Personal Data of the Republic of Lithuania' (*Teisės Aktų Registras*, 16 July 2018) <https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/VCRurdZydD> accessed 20 October 2018.

267 DLA Piper (n 31) 334-345; Baker McKenzie (n 175) 10-11.

268 DLA Piper (n 31) 346-349.

269 Idem at 350-353.

270 Idem at 354-357.

271 Idem at 358-363.

272 Idem at 364-377; Baker McKenzie (n 175) 11-12.

273 DLA Piper (n 31) 378-384; Data Protection Office, 'Data Protection Act 2017' (*Data Protection Office*, 2017) <http://dataprotection.govmu.org/English/Legislation/Pages/Data-Protection-Act-2017-.aspx > accessed on 4 October 2018.

274 DLA Piper (n 31) 385-390.

	Protection of Personal Data held by Private Parties, effective since 2011 ('Regulations') • Privacy Notice Guidelines effective since 2013 ('Guidelines')		
Monaco[275]	Law No. 1.165 of 23 December 1993 on Personal Data Protection, as modified from time to time	Provisions of the Personal Data Protection Law apply	Yes
Montenegro[276]	Law on Protection of Personal Data 2008	• General data protection rules apply • The Law on Electronic Communications 2013 applies to operators who retain users' location and traffic data	Yes
Morocco[277]	Law No. 09-08 on the Protection of Individuals in relation to the Processing of Personal Data, and its implementation Decree	General principles of data protection apply	Yes
Netherlands[278]	Implementation of the General Data Protection Regulation Act 2018	Telecommunications Act	Yes
New Zealand[279]	• Privacy Act 1993 • Sector-specific Codes	General guidelines on online privacy protection by New Zealand Privacy Commissioner	Yes
Nigeria[280]	No comprehensive legislative framework on data protection • Sector-specific laws • Guidelines on Data Protection issued by the National Information Technology Development Agency (currently under revision)	General principles relating to the right to privacy apply	Sector-specific regulatory bodies exist
Norway[281]	Personal Data Act of 15 June 2018 No. 38	• Regulation relating to Electronic Communications Networks and Electronic Communications Services of 16 February 2004 No. 401	Yes

275 Idem at 391-394.
276 Idem at 395-399.
277 Idem at 400-403.
278 Idem at 404-413; Baker McKenzie (n 175) 12.
279 DLA Piper (n 31) 414-419.
280 Idem at 420-426.
281 Idem at 427-436; AS Wiersholm (n 179).

		• The Electronic Communications Act of 4 July 2003 No. 83	
Pakistan[282]	None	None	None
Panama[283]	• Law No. 51 of 22 July 2008, as amended • Executive Decree No. 40 of 19 May 2009	None	Yes
Philippines[284]	Data Privacy Act of 2012	None	Yes
Poland[285]	Personal Data Protection Act of 10 May 2018	Telecommunications Act of 16 July 2014, as amended	Yes
Portugal[286]	GDPR	Law No. 41/2004 of 18 August (Processing of Personal Data and privacy protection in Electronic Communications), as amended	Yes
Qatar[287]	Law No. 13 of 2016 Concerning Personal Data Protection	None (except where children are concerned)	Yes (Ministry authority)
Romania[288]	Law No. 190/2018 for the application of GDPR	Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector	Yes
Russia[289]	• Federal Law No. 152-FZ of 27 July 2006 on Personal Data, as amended • Federal Law No. 149-FZ of 27 July 2006 on Information, Information Technology and the Protection of Information • Sector-specific legislation	None	Yes
Saudi Arabia[290]	Sector-specific legislation	None	None (sector-

282 DLA Piper (n 31) 437-439.
283 Idem at 440-443.
284 Idem at 444-450.
285 Idem at 451-464; Baker McKenzie (n 175) 5.
286 DLA Piper (n 31) 465-477.
287 Idem at 478-481.
288 Idem at 482-495.
289 Idem at 496-500; The Federal Service for Supervision of Communications, Information Technology, and Mass Media, 'Federal Constitutional Laws and Federal Laws' (*Federal Service for Supervision of Communications, Information Technology, and Mass Media*, 2018) <http://eng.pd.rkn.gov.ru/legislation_of_the_russian_federation/federal_constitutional_laws_and_federal_laws/> accessed 6 October 2018.
290 DLA Piper (n 31) 501-503.

			specific regulatory bodies available)
Serbia[291]	Law on Protection of Personal Data, as amended	General data protection rules apply. The Law on Electronic Communications, as amended is applicable to publicly available telecommunication service providers.	Yes
Seychelles[292]	Data Protection Act 9 of 2003 (not yet in force)	None	Not yet established
Singapore[293]	Personal Data Protection Act 2012	General data protection rules apply	Yes
Slovak Republic[294]	Act No. 18/2018 Coll. On the Protection of Personal Data	Act No. 351/2011 Coll. on Electronic Communications, as amended (applicable to electronic communications sector)	Yes
Slovenia[295]	GDPR	Electronic Communications Act	Yes
South Africa[296]	Protection of Personal Information Act 4 of 2013 (not yet fully operational)	None (however future regulations may be issued by Information Regulator to address online privacy matters)	Not yet operational
South Korea[297]	• Personal Information Protection Act • Sector-specific legislation	• Act on Promotion of Information and Communication Network Utilization and Information Protection, etc. • Act on the Protection, Use, etc. of Location Information	Yes
Spain[298]	GDPR	• Act on the Information Society Services and e-Commerce, as amended in March 2012 • Guidance Notes issued by the Spanish Data Protection Commissioner's Office	Yes

291 Idem at 504-507.
292 Idem at 508-512.
293 Idem at 513-517.
294 Idem at 518-524; Kinstellar, 'Data Protected –Slovakia' (*Linklaters*, July 2018) <https://www.linklaters.com/en/insights/data-protected/data-protected---slovakia> accessed 6 October 2018.
295 DLA Piper (n 31) 525-534; Baker McKenzie (n 175) 24.
296 DLA Piper (n 31) 535-539.
297 Idem at 540-548.
298 Idem at 549-558; Baker McKenzie (n 175) 24-25.

Sweden[299]	Data Protection Act (2018:218)	Electronic Communications Act (2003:389), as amended	Yes
Switzerland[300]	• Federal Act on Data Protection • Ordinance to the Federal Act on Data Protection • Ordinance on Data Protection Certification • Sector-specific legislation	• General data protection rules under Federal Act on Data Protection apply • Telecommunications Act regulates use of cookies	Yes
Taiwan[301]	Personal Data Protection Law 2010, as amended	General data protection rules under the Law apply	Various Ministries are competent authorities
Thailand[302]	Sector-specific legislation	None	None
Trinidad and Tobago[303]	Data Protection Act, 2011 (not fully operational)	None	Yes
Turkey[304]	• Law on the Protection of Personal Data No. 6698, and its Regulations • Sector-specific law	Electronic Communications Law No. 5809 applies where traffic data is processed by a telecommunications operator.	Yes
United Arab Emirates – Dubai (DIFC)[305]	• Data Protection Law 2007, as amended • Data Protection Regulations issued by the Commissioner of Data Protection	General data protection rules apply	Yes
UAE – General[306]	Sector-specific legislation including: • The Constitution of the UAE • Federal Law No 3 of 1987 the Penal Code • Federal Law 5 of 2012 on Combatting Cybercrime • Federal Law by Decree No. 3 of 2003 regarding the Organisation of the Telecommunications Sector	Provisions of the Penal Code apply	
Ukraine[307]	Law No. 2297-VI on Protection of Personal Data, as	General data protection rules apply insofar that	Yes

299 DLA Piper (n 31) 559-569.
300 Idem at 570-576.
301 Idem at 577-580.
302 Idem at 581-583.
303 Idem at 584-588.
304 Idem at 589-594.
305 Idem at 595-601.
306 Idem at 602-607.

	amended	online activities concern the processing of personal data	
United Kingdom[308]	Data Protection Act 2018	Privacy and Electronic Communications (EC Directive) Regulations deals with the collection of location and traffic data by public ECSPs and the use of cookies	Yes
United States[309]	Privacy Act of 1974. There are sector-specific laws and each state has its own state laws	No federal regulation. Online privacy is regulated in certain states in the United States	Yes (Federal Trade Commission regarded as competent authority)
Uruguay[310]	Law No. 18.331 on Protection of Personal Data and 'Habeas Data' Action	None	Yes
Zimbabwe[311]	• Access to Information and Protection of Privacy Act • Sector-specific legislation	None	None (certain governmental bodies available)

307 Idem at 608-614.
308 Idem at 615-627.
309 Idem at 628-632.
310 Idem at 633-635.
311 Idem at 636-638.

9 BIBLIOGRAPHY

1. International treaties

Universal Declaration of Human Rights (adopted 10 December 1948) UNGA Res 217 A(III).

International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

Statue of the International Court of Justice of 1945.

2. Regional treaties

a. European treaties

Charter of Fundamental Rights of the European Union [2012] OJ C 326/02 (EU Charter of Fundamental Rights).

European Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended).

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

b. African region

African Charter on Human and Peoples' Rights (adopted 27 June 1981, entered into force 21 October 1986) (1982) 21 ILM 58.

Africa Union Convention on Cyber Security and Personal Data Protection (adopted by the Twenty-third Ordinary Session of the Assembly on 27 June 2014, not yet in force).

c. Other regional treaties

American Declaration of the Rights and Duties of Man, OAS Res XXX adopted by the Ninth International Conference of American States (1948) reprinted in Basic

Documents Pertaining to Human Rights in the Inter-American System OEA/Ser L V /II.82 Doc 6 Rev 1 at 17 (1992).

American Convention on Human Rights (adopted 22 November 1969, entered into force 18 July 1978) (1969) 1144 UNTS 123.

3. Other international organisations

a. United Nations Documents

United Nations General Assembly Resolution 68/167 on the Right to Privacy in the Digital Age (18 December 2013).

United Nations General Assembly Resolution 45/95 on the Guidelines for the Regulation of Computerized Personal Data Files (14 December 1990) UN Doc E/CN.4/1990/72.

UN Human Rights Council 'Report of the Special Rapporteur on the Right to Privacy' (2018) UN Doc A/HRC/37/62 (advance unedited version).

b. Other instruments

Asia-Pacific Economic Cooperation (APEC) 'APEC Privacy Framework' (published by APEC in August 2017) (2015) APEC #217-CT-01.9

Organisation for Economic Co-Operation and Development (OECD), 'Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data' (adopted 23 September 1980, amended 11 July 2013) OECD/LEGAL/0188 (OECD Guidelines).

4. International Court of Justice Cases

North Sea Continental Shelf Cases 1969 ICJ Reports 3

Fisheries Jurisdiction case 1974 ICJ Reports 3

5. European legislation

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal

data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ 2016 L 119/1.

6. National legislation

Angola

Lei No. 22/11 da Protecção de Dados Pessoais de 17 de Junho.

Lei No. 7/17 de Protecção das Redes e Sistemas Informáticos de 16 de Fevereiro.

Lei No. 23/11 das Comunicações Electrónicas e dos Serviços da Sociedade de Informação de 20 de Junho.

Argentina

Personal Data Protection Law No. 25,326 of October 2000.

Australia

Privacy Act 1988.

Information Privacy Act 2014.

Austria

Federal Act concerning the Protection of Personal Data (Datenschutzgesetz), Federal Law Gazette I No. 165/1999 as last amended by the Data Protection Amendment Act 2018, Federal Law Gazette I No. 120/2017.

Federal Act enacting the Telecommunications Act, Federal Law Gazette I No. 70/2003, as amended by Federal Law Gazette I No. 44/2014.

Belarus

Law on Information, Informatisation and Information Protection of 10 November 2008 No. 455 Z.

Belgium

Wet van 30 Juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens, Belgisch Staatsblad 5 September 2018, p. 68616.

Wet van 13 Juni 2005 betreffende de elektronische communicatie, Belgisch Staatsblad 20 Juni 2005, p. 28070.

Bermuda

Personal Information Protection Act 2016.

Bosnia and Herzegovina

Law on Protection of Personal Data ("Official Gazette of Bosnia and Herzegovina" No. 49/06).

Law on Amendments to the Law on the Protection of Personal Data ("Official Gazette of Bosnia and Herzegovina" No. 76/11 and 89/11).

Bulgaria

Law for Protection of Personal Data (State Gazette No.1 of 4 January 2002).

Electronic Commerce Act (State Gazette No. 51 of 23 June 2006).

Canada

Personal Information Protection and Electronic Documents Act, Statutes of Canada 2000, c. 5.

Personal Information Protection Act, Statutes of Alberta 2003, c. P-6.5.

Personal Information Protection Act, Statutes of British Colombia 2003, c. 63.

Act Respecting the Protection of Personal Information in the Private Sector, Revised Statutes of Quebec, c. P-39.1.

Cape Verde

Lei nº 133/V/2001, de 22 de Janeiro, estabelece o regime jurídico de tratamento de dados pessoais a pessoas singulars.

Lei nº 41/VIII/2013 Regime Jurídico Geral da Protecção de Dados Pessoais das Pessoas Singulares.

Lei nº 134/V/2001, de 20 Dezembro 2000, estabelece o regime, jurídico de tratamento de dados pessoais no sector das telecomunicações.

Cayman Islands

Data Protection Law, 2017.

China (Peoples' Republic of)

Cyber Security Law of the People's Republic of China (2017).

The Decision of the Standing Committee of the National People's Congress on Strengthening Network Information Protection (2012).

National Guiding Technical Documents of the People's Republic of China on Information Security Technology – Guideline for Personal Information Protection within Information System for Public and Commercial Services (GB/Z 28828-2012)**.**

Law of the People's Republic of China on the Protection of Consumer Rights and Interests, as amended in October 25, 2013.

Administrative Provisions on Administration of Information Services of Mobile Internet Application Programs (2016).

Costa Rica

Law No. 8968, *Protection in the Handling of the Personal Data of Individuals.*

Croatia

Law on the Implementation of the General Data Protection Regulation ('Official Gazette of the Republic of Croatia', No. 42/2018).

Electronic Communications Act ('Official Gazette of the Republic of Croatia', Nos. 73/2008, 90/2011, 133/2012, 80/2013 and 71/2014).

Cyprus

Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of Such Data of 2018 (Law 125(I)/2018).

The Regulation of Electronic Communications and Postal Services Law of 2004 to 2016.

Czech Republic

Act No. 127/2005 Coll. on Electronic Communications.

Denmark

Act no. 502 of 23 May 2018 on supplementary provisions to the Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

Act on Electronic Communications Services and Networks 2011.

Executive Order on Information and Consent Required in Case of Storing and Accessing Information in End-user Terminal Equipment 2011.

Egypt

Constitution of the Arab Republic of Egypt 2014.

Egyptian Civil Code of 1949.

Finland

Law on Electronic Communications Services 917/2014.

France

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

Code des postes et des communications électroniques.

Germany

Federal Data Protection Act of 30 June 2017, *Bundesgesetzblatt* I p. 2097.

Ghana

Data Protection Act 843 of 2012.

Gibraltar

Data Protection Act 2004.

The Communications (PD&P) Regulations 2006.

Greece

Law 2472/1997 on the Protection of Individuals with regard to the Processing of Personal Data.

Guernsey

Data Protection (Bailiwick of Guernsey) Law, 2017.

Data Protection (Commencement, Amendment and Transitional) (Bailiwick of Guernsey) Ordinance, 2018.

Data Protection (Law Enforcement and Related Matters) (Bailiwick of Guernsey) Ordinance, 2018.

European Communities (Implementation of Privacy) Directive (Guernsey) Ordinance 2004.

Honduras

Constitución de la República de Honduras, 1982.

Decreto No. 62-2004, Ley del Registro Nacional de las Personas (Publicado en el Diario Oficial La Gaceta No. 30,390 el 15 de Mayo de 2004).

Decreto No. 170-2006, Ley de Transparencia y Acceso a la Información Pública (Publicada en el Diario Oficial La Gaceta el 30 de Diciembre de 2006).
Acuerdo No. IAIP-0001-2008, Reglamento de la Ley de Transparencia y Acceso a la Información Pública (Publicado en el Diario Oficial La Gaceta el 6 de Marzo de 2008).

Hong Kong

The Personal Data (Privacy) Ordinance (Cap. 486 of the Laws of Hong Kong).

Hungary

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information.

2018. évi XIII. Törvény –Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény jogharmonizációs célú módosításáról.

2018. évi XXXVIII. Törvény - Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról.

Act C of 2003 on Electronic Communications.

Iceland

Act No. 90/2018 on Data Protection and the Processing of Personal Data.

India

Personal Data Protection Bill, 2018.

Indonesia

Law of the Republic of Indonesia No. 11 of 2008 Concerning Electronic Information and Transactions, as amended by Law of the Republic of Indonesia No. 19 of 2016 on the Amendment to Law No. 11 of 2008 on Electronic Information and Transactions.

Regulation of the Government of the Republic of Indonesia No. 82 of 2012 Concerning Provisions of Electronic systems and Transactions.

Minister of Communications and Informatics Regulation No. 20 of 2016 regarding the Protection of Personal Data in an Electronic System.

Ireland

Data Protection Act, 2018.

European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011, Statutory Instrument No. 336 of 2011.

Israel

Protection of Privacy Law, 5741-1981.

Italy

Legislative Decree No. 101/2018 concerning the provisions for the adaptation of the national legislation to the Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and rules to the free movement of such data.

Legislative Decree No. 196/2003 concerning the Personal Data Protection Code.

Japan

Protection of Personal Information Act No. 57 of 2003, as last amended in December 2016.

Jersey

Data Protection (Jersey) Law 2018.

Latvia

Law of 2018 on Personal Data Processing.

Law of 4 November 2004 on Information Society Services.
Law of 28 October 2004 on Electronic Communications.

Lesotho

Data Protection Act 2013.

Lithuania

Law on Legal Protection of Personal Data of the Republic of Lithuania of June 11, 1996 No. I-1374 (as amended on July 16, 2018 Law No.XIII-1426).

Luxembourg

Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et mise en oeuvre du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État.

Macau

Law No. 8/2005 of August 22, on the Protection of Personal Data.

Macedonia

The Law on Personal Data Protection (Official Gazette of the Republic of Macedonia, No. 7/2005, 103/2008, 124/2008, 124/2010, 135/2011 and 43/2014).

Madagascar

Loi N° 2014 – 038 Sur la protection des données à caractère personnel.

Malaysia

Personal Data Protection Act 2010.

Malta

Data Protection Act (Cap. 586).

Processing of Personal Data (Electronic Communications Sector) Regulations (Subsidiary Legislation 586.01).

Mauritius

Data Protection Act 20 of 2017.

Mexico

Federal Law on the Protection of Personal Data held by Private Parties, effective since 5 July 2010.

The Regulations to the Federal Law on the Protection of Personal Data held by Private Parties, effective since 21 December 2011.

Privacy Notice Guidelines, effective since 17 April 2013.

Monaco

Law No. 1.165 of 23 December 1993 on Personal Data Protection.

Montenegro

Law on Protection of Personal Data 2008 (Official Gazette of Montenegro Nos. 79/2008, 70/2009 and 44/2012).

The Law on Electronic Communications ('Official Gazette of Montenegro', nos. 40/2013 and 56/2013).

Morocco

Law No. 09-08 of 18 February 2009 relating to the protection of individuals with regard to the processing of personal data.

Decree 2-09-165 of 21 May 2009 for the application of Law No. 09-08 on the protection of individuals with regard to the processing of personal data.

The Netherlands

Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119), *Staatsblad* 2018, 144.

Wet op de Telecommunicatievoorzieningen, *Staatsblad* 1988, 520.

New Zealand

Privacy Act 1993.

Norway

Personal Data Act 15 of June 2018 No. 38.

Electronic Communications Act of 4 July 2003 No. 83.

Regulation relating to Electronic Communications Networks and Electronic Communications Services of 16 February 2004 No. 401.

Panama

Law No. 51 of 22 July 2008, as amended by Law No. 82 of 9 November 2012.

Executive Decree No. 40 of 19 May 2009.

Philippines

Republic Act No. 10173 (2012), Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes.

Poland

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dziennik Ustaw 2018, poz. 1000.

Ustawa z dnia 16 lipca 2004 r. Prawo Telekomunikacyjne, Dziennik Ustaw 2004 Nr. 171, poz. 1800.

Portugal

Lei n.º 41/2004 de 18 de Agosto (Tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas).

Qatar

Law No. 13 of 2016 Concerning Personal Data Protection

Romania

Law No. 190/2018 on the measures for the application of 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 published in the Official Gazette No. 651 of 26 July 2018.

Law No. 506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector published in the Official Gazette No. 1101 of 25 November 2004.

Russia

Federal Law of 27 July 2006 No. 152-FZ “on Personal Data”.

Federal Law of 21 July 2014 No. 242-FZ “On amendments to certain legislative acts of the Russian Federation to clarify the procedure of personal data processing in information and telecommunication networks”.

Federal Law of 27 July 2006 No. 149-FZ “On Information, Information Technology, and Protection of Information”.

Serbia

Law on Protection of Personal Data ('Official Gazette of the Republic of Serbia', nos. 97/2008, 104/2009, 68/2012 and 107/2012).

Law on Electronic Communications ('Official Gazette of the Republic of Serbia', nos. 44/2010, 60/2013 and 62/2014).

Seychelles

Data Protection Act 9 of 2003.

Singapore

Personal Data Protection Act 2012 (Cap. 26).

Slovak Republic

Act No. 18/2018 Coll. On the Protection of Personal Data.

Act No. 351/2011 Coll. on Electronic Communications.

Slovenia

Electronic Communications Act (Official Gazette of the Republic of Slovenia, Nos. 109/12, 110/13, 40/14 – ZIN-B, 54/14 – Rev. US, 81/15 and 40/17).

South Africa

Protection of Personal Information Act 4 of 2013.

South Korea

Personal Information Protection Act (Act No. 10465 of March 29, 2011, as amended up to Act No. 14839 of July 26, 2017).

Act on the Promotion of Information and Communications Network Utilization and Information Protection, etc. (Act No. 3848 of May 12, 1986, as amended up to Act No. 14080 of March 22, 2016).

Act on the Protection, Use, etc. of Location Information (Act No. 7372 of January 27, 2005, as amended up to Act No. 14224 of May 29, 2016).

Spain

Act 34/2002 of 11 July on Information Society Services and Electronic Commerce.

Sweden

Lag (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning.

Lag (2003:389) om elektronisk kommunikation.

Switzerland

Federal Act of 19 June 1992 on Data Protection.

Ordinance of 14 June 1993 to the Federal Act on Data Protection.

Ordinance of 28 September 2007 on Data Protection Certification.

Telecommunications Act of 30 April 1997.

Taiwan

Personal Data Protection Law 2010.

Trinidad and Tobago

Data Protection Act 2011.

Turkey

Law on the Protection of Personal Data No. 6698 of 7 April 2016.

Electronic Communications Law No. 5809 of 5 November 2008.

United Arab Emirates – Dubai (Dubai International Financial Centre)

Data Protection Law, DIFC Law No. 1 of 2007, amended by Data Protection Law Amendment Law, DIFC Law No. 5 of 2012.

United Arab Emirates – General

The Constitution of the United Arab Emirates of 1971, as amended.

Federal Law No. 3 of 1987 Concerning Promulgating Penal Code.

Federal Law No. 5 of 2012 on Combatting Cybercrimes.

Federal Law by Decree No. 3 of 2003 regarding the Organisation of the Telecommunications Sector.

Ukraine

Law of Ukraine No. 2297-VI of 1 June 2010 on Protection of Personal Data.

United Kingdom

Data Protection Act 2018.

Privacy and Electronic Communications (EC Directive) Regulations 2003.

United States

Privacy Act of 1974, 5 United States Code.

Uruguay

Law No 18.331 on Protection of Personal Data and 'Habeas Data' Action of 11 August 2008.

Zimbabwe

Access to Information and Protection of Privacy Act [chapter 10:27].

7. Books and articles

Baker McKenzie, 'GDPR National Legislation Survey, 4.0' (Baker McKenzie, August 2018).

Bygrave L, 'An international data protection stocktake @ 2000, Part 2: core principles of data protection instruments' (2001) 7 Privacy Law & Policy Reporter 169-178.

Bygrave L, 'The Place of Privacy in Data Protection Law' (2001) University of New South Wales Law Journal.

Caudill EM and Murphy PE, 'Consumer Online Privacy: Legal and Ethical Issues' (2009) 19(1) Journal of Public Policy & Marketing.

Cooper ER and Raul AC, 'APEC Overview' in AC Raul (ed), *The Privacy, Data Protection and Cybersecurity Law Review* (4th ed, Law Business Research Ltd, London 2017).

De Hert P and Gutwirth S, 'Privacy, data protection and law enforcement. Opacity of the individual and transparency of power' in E Claes, A Duff and S Gutwirth (eds.), *Privacy and the Criminal Law* (Intersentia, 2006).

DLA Piper, 'Data Protection Laws of the World: Full Handbook' (DLA Piper, October 2018) <https://www.dlapiperdataprotection.com/index.html.>accessed 11 October 2018.

Dugard J, *International Law: A South African Perspective* (4th edn, Juta 2011).

Forde A, ‘The Conceptual Relationship between Privacy and Data Protection’ (2016) 1 Cambridge Law Review.

Greenleaf G, ‘Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey’ (2017) 145 Privacy Laws & Business International Report.

Lindsay D, ‘An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law’ (2005) 29(1) Melbourne University Law Review.

Lynskey O, ‘Deconstructing data protection: the ‘added-value’ of a right to data protection in the EU legal order’ (2014) 63(3) International and Comparative Law Quarterly.

Mayer JR and Mitchell JC, ‘Third-Party Web Tracking: Policy and Technology (2012 IEEE Synopsis on Security and Privacy, San Francisco, May 2012).

O’Connor P, ‘An International Comparison of Approaches to Online Privacy Protection’ (Information and Communication Technologies in Tourism, Vienna, 2005).

OECD, *The OECD Privacy Framework* (OECD Publishing 2013) Chapter 4 The evolving privacy landscape: 30 years after the OECD Privacy Guidelines (2011).

Purtova N, ‘Private Law Solutions in European Data Protection: Relationship to Privacy, and Waiver of Data Protection Rights’ (2010) 28(2) Netherlands Quarterly of Human Rights.

Rachovitsa A, ‘Engineering and lawyering privacy by design: understanding online privacy both as a technical and an international human rights issue’ (2016) 24 International Journal of Law and Information Technology.

Rengel A, ‘Privacy as an International Human Right and the Right to Obscurity in Cyberspace’ (2014) 2(2) Groningen Journal of International Law.

Roos A, ‘Core principles of data protection law’ (2006) 39(1) The Comparative and International Law Journal of Southern Africa.

Rotenberg M and Knight A, Privacy and Human Rights 2006: An International Survey of Privacy Laws and Developments (1st edn, Electronic Privacy Information Center, Washington and Privacy International, London 2007).

Shepardson D, 'Trump signs repeal of U.S. broadband privacy rules' (*Reuters*, 4 April 2017) <https://www.reuters.com/article/us-usa-internet-trump/trump-signs-repeal-of-u-s-broadband-privacy-rules-idUSKBN1752PR>accessed 6 March 2018.

Tan JG, 'A Comparative Study of the APEC Privacy Framework –A New Voice in the Data Protection Dialogue?' (2008) 3 Asian Journal of Comparative Law.

Tang Z, Hu Y and Smith MD, 'Gaining Trust through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor' (2008) 24(4) Journal of Management Information Systems.

Zalnieriute M, 'An international constitutional moment for data privacy in the times of mass-surveillance' (2015) International Journal of Law and Information Technology 1-35.

8. Websites

APEC, 'Member Economies' (APEC, 2017) <https://apec.org/About-Us/About-APEC/Member- Economies> accessed 6 June 2018.

AU, 'List of countries which have signed, ratified/acceded to the African Union Convention on Cyber Security and Personal Data Protection' obtained from <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed on 6 June 2018.

Boonklomjit H, Rerknithi N, Gamvros A and Kwok R, 'Overview of Thailand Draft Personal Data Protection Act' (Norton Rose Fulbright, 6 August 2018) <https://www.dataprotectionreport.com/2018/08/overview-of-thailand-draft-personal-data-protection-act/> accessed 20 October 2018.

Council of Europe, 'Chart of signatures and ratifications of Treaty 108' (Council of Europe, 27 June 2018) <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=XOI51XuE> accessed 27 June 2018.

Data Protection Office, 'Data Protection Act 2017' (*Data Protection Office*, 2017) <http://dataprotection.govmu.org/English/Legislation/Pages/Data-Protection-Act-2017-.aspx > accessed on 4 October 2018.

English Oxford Living Dictionaries, 'Definition of *online*' (*Oxford University Press*, 2018) <https://en.oxforddictionaries.com/definition/online> accessed 20 June 2018.

European Commission, 'Guide to the EU-U.S. Privacy Shield' (European Commission, 2016) available on <https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/eu-us-privacy-shield_en> accessed 10 June 2018.

Gianni, Origoni, Grippo, Cappelli & Partners (October 2018) 'Data Protected – Italy) <https://www.linklaters.com/en/insights/data-protected/data-protected---italy> accessed 4 October 2018.

International Association of Privacy Professionals, 'Glossary of Privacy Terms' (IAPP, 2018) <https://iapp.org/resources/glossary/> accessed 10 May 2018.

International Conference of Data Protection and Privacy Commissioners (ICDPPC), 'Mission and Vision' obtained from <https://icdppc.org/the-conference-and-executive-committee/strategic-direction-mission-and-vision/> accessed on 3 June 2018.

International Conference of Data Protection and Privacy Commissioners (ICDPPC), 'Home Page' obtained from <https://icdppc.org> accessed on 3 June 2018.

Kinstellar, 'Data Protected –Slovakia' (*Linklaters*, July 2018) <https://www.linklaters.com/en/insights/data-protected/data-protected---slovakia> accessed 6 October 2018.

Ministry of Justice of the Republic of Latvia, 'Latvia is the first among the Baltic States to adopt the Personal Data Processing Law' (*Ministry of Justice of the Republic of Latvia*, 21 June 2018) <https://www.tm.gov.lv/en/news/latvia-is-the-first-

among-the-baltic-states-to-adopt-the-personal-data-processing-law> accessed on 14 October 2018.

OECD, 'List of OECD Member countries –Ratification of the Convention on the OECD' (OECD, 2018) <http://www.oecd.org/about/membersandpartners/list-oecd-member-countries.htm> accessed 6 June 2018.

Personal Information Protection Commission Japan 'Laws and Policies' (*Personal Information Protection Commission, Japan*, 2018) <https://www.ppc.go.jp/en/legal/> accessed 16 October 2018.

Persónu Vernd, 'General Introduction' (*Persónu Vernd*, 2018) <https://www.personuvernd.is/information-in-english/greinar/nr/437> accessed on 14 October 2018.

Regidi A, 'Data Protection Bill Series: Quick Overview of India's Draft Data Protection Law' (*Tech2*, 28 July 2018) <https://www.firstpost.com/tech/news-analysis/data-protection-bill-series-quick-overview-of-indias-draft-data-protection-law-4841321.html> accessed 14 October 2018.

Republik Österreich Datenschutzbehörde, 'Data protection law in Austria' (*Republik Österreich Datenschutzbehörde*, 2018) <https://www.dsb.gv.at/gesetze-in-osterreich> accessed 1 October 2018.

Teisės Aktų Registras, 'Law on Legal Protection of Personal Data of the Republic of Lithuania' (*Teisės Aktų Registras*, 16 July 2018) <https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/VCRurdZydD> accessed 20 October 2018.

The Federal Service for Supervision of Communications, Information Technology, and Mass Media, 'Federal Constitutional Laws and Federal Laws' (*Federal Service for Supervision of Communications, Information Technology, and Mass Media*, 2018) <http://eng.pd.rkn.gov.ru/legislation_of_the_russian_federation/federal_constitutional_laws_and_federal_laws/> accessed 6 October 2018.

United States of America Department of Commerce, ‘EU-U.S. Privacy Shield’ (Department of Commerce) <https://www.commerce.gov/tags/eu-us-privacy-shield> accessed 10 June 2018.

Wiersholm AS, ‘Data Protected – Norway’ (*Linklaters*, September 2018) <https://www.linklaters.com/en/insights/data-protected/data-protected---norway> accessed 4 October 2018.