A Comparative Analysis of Privacy Standards in the OECD Guidelines, the E.U., the Canada and Brazil

Regina Marin
Instituto Federal de Educação, Ciência e Tecnologia de São Paulo - IFSP
Campinas, Brazil
regina.marin@ifsp.edu.br

***Abstract*— The necessity of a legal protection has become an important issue, due to different types of privacy violations. Many countries are seeking to protect individuals' privacy through constitutional laws, regulations and court examinations. However, there are significant differences in the ways in which nation implemented the protection of privacy and personal data. The aim of this paper is to determine the extent to which the concepts and principles are consistent by four different privacy standards - the OECD Guidelines, the E.U., the Canada and Brazil**.

Keywords—standards; privacy; the brazilian civil rights framework for the internet

I. INTRODUCTION

One of the most significant concepts in the contemporary democratic societies is privacy. Privacy is a multidimensional concept that encompasses different notions concerning personal information, freedom of intrusion, and protection from searches and surveillance. The value of privacy is so relevant that is recognized as a basic human right in Article 12 of the United Nations' Universal Declaration of Human Rights [13]: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attack."

Although researchers and other professionals have been working to increase individuals' privacy, violations in people's activities and business still remain an important issue. A privacy violation occurs when personal information is improperly or unauthorized collected, used, or disseminated. Often, when a privacy violations occur, victims are spoiled with embarrassment, mental distress, reputation problems, financial loss and other disadvantages.

To protect individuals' privacy, legislation and other legal implementation of data protection vary across the globe. In this context, three standards have influenced modern worldwide privacy laws: the Organization for Economic Co-operation and Development (OECD), the Canadian Standards Association Model Code, and the European Data Protection Directive 95/46/EC. Like these traditional regulations, Brazil also have established a Federal Law No. 12.965/2014 providing general principles for storage, use, and disclosure of data collected on-line.

The paper is organized as follows. Section II presents the OECD guidelines. Section III reviews the Canadian Standards Association Model Code. Section IV describes European Data Protection Directive 95/46/EC and the current General Data Protection Regulation. Section V describes The Brazilian Civil Rights Framework for the Internet. Section VI presents a functional comparative analysis between these different privacy standards. We finally conclude in section VII.

II. OECD GUIDELINES

In 1980, the Organization for Economic Co-operation and Development (OECD) adopted principles for protecting personal data, including how data would be protected in cross border transactions among OECD members [5]. These principles are based on the Fair Information Practice Principles (FIPPs), and were updated in 2013 in a document titled The OECD Privacy Framework [10]. The revised OECD guidelines include additional obligations on data controller operations, audit processes, and more emphasis on the controller's accountability. The following eight basic principles are extracted from the OECD 2013 guidelines [10], which are known as Guidelines on the Protection of Privacy and Transborder Flows of Personal Data:

OECD.1. Collection Limitation: there should be limits to the collection of personal data and any data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

OECD.2. Data Quality: personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

OECD.3. Purpose Specification: the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

OECD.4. Use Limitation: personal data should not be disclosed, made available or otherwise used for purposes other

than those specified in accordance with Purpose Specification item, except: a) with the consent of the data subject; or b) by the authority of law.

OECD.5. Security Safeguards: personal data should be protected by reasonable security safeguards against risks of loss or unauthorised access, destruction, use, modification or disclosure of data.

OECD.6. Openness: there should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

OECD.7. Individual Participation: individuals should have the right to:

- obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
- have communicated to them, the data relating to them (i) within a reasonable time; (ii) at a charge, if any, that is not excessive; (iii) in a reasonable manner; and (iv) in a form that is readily intelligible to them;
- be given reasons if a request made under items (a) and (b) are denied, and to be able to inquire such denial; and
- inquire data relating to them and, if the inquire is successful, have the data erased, rectified, completed or amended.

OECD.8. Accountability: a data controller should be accountable for complying with measures which give effect to these principles.

III. Canadian Standards Association Model Code – CSAC

Canada has a well-accepted model code of conduct with respect to privacy, called the Canadian Standards Association Model Code - CSAC for the Protection of Personal Information [7]. It was developed based on the existing OECD Privacy Guidelines [5] by the Canadian Standards Association, which is Canada's major organization for standards development and certification. The CSAC is the basis of the Canada's federal law on the topic of data privacy, called Personal Information Protection and Electronic Documents Act (PIPEDA).

The CSAC was adopted by the Government of Canada in 1996 and reaffirmed in 2001. The following describes the ten privacy principles of the CSAC [7]:

CSAC.1. Accountability: an organization is responsible for the personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance in relation to the privacy principles.

CSAC.2. Identifying Purposes: the purpose for which personal information is collected shall be identified by the organization at or before the time the information is collected.

CSAC.3. Consent: the knowledge and consent of the individual are required for the collection, use or disclosure of personal information.

CSAC.4. Limiting Collection: the collection of personal information shall be limited to the purposes identified by the organization. Information shall be collected in a fair and lawful means.

CSAC.5. Limiting Use, Disclosure, and Retention: personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by the law. In addition, personal information shall be retained only as long as necessary for the fulfilment of those purposes.

CSAC.6. Accuracy: personal information shall be as accurate, complete, and up-to-date as is necessary for the intended purposes

CSAC.7. Safeguards: security safeguards appropriated to the information sensitivity shall be used to protect personal information.

CSAC.8. Openness: an organization shall make readily available to individuals specific information about its policies and practices related to the management of personal information.

CSAC.9. Individual Access: upon request, an individual shall be informed of the existence, use and disclosure of her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

CSAC.10. Challenging Compliance: An individual shall be able to inquire the organization's compliance with respect to any aspect of the CSAC Code, and the organization must respond to all inquiries and complaints.

IV. European Data Protection Directive 95/46/EC and The General Data Protection Regulation

In the European Union (E.U.), personal data protection is currently described by a set of regulations centred around the Data Protection Directive 95/46/EC (i.e., Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data) [11].

The Directive European (DE) specifies extensive data protection goals to be reached by institutions, organization and people within E.U., imposing broad obligations on those who collect and control personal data. Each E.U. member must implement the Directive, but has a certain degree of freedom on how it is implemented. Examples of implementations of the Directive are the Italian's Codice in materia di protezione dei dati personali [3], the French's Loi relative `a l'informatique, aux fichiers et aux libertés [9], and the United Kingdom's Data

protection act [8]. The current Directive only applies to organizations that either process personal information of European citizens or makes use of information systems within the E.U. The following describes the nine principles of the Directive 95/46/EC [14, 4]:

DE.1. Intention and Notification: the processing of personal data must be reported in advance to the Data Protection Authority or a personal data protection official, unless processing has been exempted from notification.

DE.2. Transparency: the person involved must be able to see who is processing her personal data and for what purpose.

DE.3. Finality: this principle corresponds the so-called Purpose Principle, which states that personal data may only be collected for specific, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.

DE.4. Legitimate Ground for Processing: the processing of personal data must be based on a foundation referred to in national legislation, such as permission, agreement, legal obligation, justified interest and such like. For special data, such as sensitive data, stricter limits prevail.

DE.5. Quality: this principle corresponds the so-called Proportionality Principle which states that the personal data must be as correct and as accurate as possible, sufficient, to the point and not excessive.

DE.6. Data Subject's Rights: the data subjects involved have the right to peruse and to correct their data as well as the right to raise objections.

DE.7. Security: providing appropriate security for personal data held within information systems is one of the cornerstones of the Data Protection Directive. Measures of technical and organisational nature suitable and proportional to the sensitivity of the data, as well as possible risks with potential harms, should be considered to avoid misuse or disclosure of personal data.

DE.8. Processing by a Processor: if processing is outsourced to a processor, it must be ensured that the processor will observe the instructions of the controller.

DE.9. Transfer of Personal Data Outside the E.U.: in principle, the traffic of personal data to a country outside the E.U. is permitted only if that country offers adequate protection.

In 2012, the European Commission proposed a reform of the E.U.'s data protection rules to cope with new technologies in social networks and cloud computing [6]. The new rules were officially released in 2016 under the name "General Data Protection Regulation" (GDPR) [12] with the enforcement beginning on May 25 2018, and is intended to replace the current Data Protection Directive [11]. The new aspects of the proposed GDPR include:

GDPR.1. Informed Consent (Art. 4), which grants individuals the right to be always informed and fully aware about what data is being processed. Moreover, consent must be specific and withdraw at any time.

GDPR.2. Transparency for Data Handling and Communication (Art. 11), which grants individuals the right to be informed on what is done with their information.

GDPR.3. The Right to Erasure (Art. 17), which grants individuals the right to request the erasure of personal data, thus avoiding further data processing.

GDPR.4 Regulation of Profiling (Art. 20), which grants individuals the right to not be characterized based on profiling.

GDPR.5. Data Protection by Design and by Default (Art. 23 (3) and (4)), inspired by the "privacy by design" approach. The aspects of privacy by design mostly stressed in the GDPR are privacy by default and privacy all along the lifecycle of the system; and

GDPR.6. Data Protection Impact Assessments (Art. 33), which have to be conducted when processing operations present specific risks to the rights and freedoms of data subjects. The risk-based approach should be an important criterion to determine obligations and safeguards for a controller and a processor.

V. The Brazilian Civil Rights Framework for the Internet (Law 12.965/2014)

In April 2014, The Brazilian Civil Rights Framework for the Internet became a law 12.965 in Brazil. The Brazilian Civil Rights Framework for the Internet (BCFI) consists of general principles such as the right to privacy, intimacy and net neutrality. The BCFI is not a data protection law, but it has a substantial portion that deals with privacy and data protection in order to ensure a set of rights and obligations for the online world. The following describes the principles of the Law 12.965 [1]:

BCFI.1. Informed Consent (Art. 7°, IX, and 16, I), the expressed consent shall be specified in a separate contractual clause for the collection, use, storage and processing of personal data.

BCFI.2. Transparency (Art. 7°, VI), clear and comprehensive information should be provided to users in the contracts of provision of services, with details on the protection scheme for connection logs and access logs of Internet applications, as well as network management practices.

BCFI.3. Purpose (Art. 7°, VIII), personal data can only be used for the purpose that is justified for gathering; specified in the contracts of provision of services or in terms of internet applications; and not prohibited by law.

BCFI.4. Information Security (Art. 10°, IV), the security and confidentiality measures and procedures shall be informed in a clear manner by the responsible for the provision of the services, and meet the standards set in regulation, in compliance with rights of confidentiality of business secrets.

BCFI.5. The Right to Sovereignty (Art. 11°), which determines the enforcement of the Brazilian law in any operation of collection, storage and treatment of records, personal data or communication by Internet connection and application providers if these operations occur in Brazil. This rule applies even if the operation is conducted by a company or

entity headquartered outside Brazil, as long as it offers services to the public in the country, or if at least one company of the same corporate group is headquartered in Brazil.

BCFI.6. Data Logs Retention (Art. 13 and Art. 15), requires that Internet connection providers retain Internet connection logs for a minimum period of 6 months to 1 year. Moreover, both articles in Paragraph 2, allow for the extension of retention periods in certain circunstances without limit the maximum time - which may be theoretically unlimited. Even thought, the law states that records must be kept confidential and security and can only be delivered to public authorities after a court order.

BCFI.7. The Right to Exclusion (Art. 7, X), the data subject can require the definitive exclusion of his/her personal data to the particular Internet application, at the end of the relation between the parties by means of a specific court order.

VI. Privacy standards Compared

This section compares and contrasts the data protection frameworks OECD (section II), CSAC (section III), Directive 95/46/EC (section IV) and the Brazilian Civil Rights Framework for the Internet (section V) to better understand the extent to which it is possible to map the classifications of regulation and implementation of data protection.

In the scope of these regulatory data protection frameworks the users' consent legitimates the use and process of personal data, as suggested by principles OECD.1, CSAC.3, ED.4., GDPR.1 and BCFI.1 The latest definition of consent is provided by the GDPR in article 25: "Consent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either by a statement or by a clear affirmative action that is the result of choice by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data" [12].

Also, these frameworks introduce distinct responsibilities between data processors and data controllers. The concepts of "controller" and "processor" appear as distinct features within OECD, Directive 95/46/EC and GDPR. The controller decides the purposes and use of the processing of personal data, while the processor processes personal data on behalf of the controller. Often, these concepts are difficult to apply in practice because of the complex relationships between them when processing personal data [2]. Conversely, the CSAC do not make a clear distinction, regarding responsibilities, between data processor and data controllers.

In the Directive 95/46/EC and the GDPR, controllers and processors are involved in the transfer of personal data to other countries outside the E.U., and both must provide an adequate level of protection according to the principle ED.9 Transfer of Personal Data Outside the E.U. Thus, the territorial space of these data protection systems Controller decides the purposes and use of the processing of personal data. Processor processes personal data on behalf of the controller extends beyond the European territory.

In order to assist the development of CSAC compliant code, a handbook called "Making the CSA privacy code work for you" was proposed. Similarly, aiming to clarify and guide the application of the Directive 95/46/EC for all member states of the E.U., representatives of Data Protection Authorities composing the European Article 29 Working Party have been providing many documents with opinions and advices on data protection and privacy since 1996.

Regarding data retention, the principle BCFI.6 imposes obligations for both Internet Service Providers (ISPs) services and Internet Application Providers that will have to assume the responsibility of keep recording of access records that may facilitate the investigation of crimes committed over the internet without disregarding privacy or the users' freedom of expression. In contrast, in Europe the Data Retention Directive (Directive 2006/24/EC) was invalidated by the decision of the Court of Justice of the European Union (CJEU) on April 2014 by allegations that it violates the right to privacy.

A comparison of the principles of OECD, CSAC, E.U. Directive 95/46/EC and GDPR, and the BCFI is proposed in the Table I.

TABLE I. Comparison of privacy standards

OECD	*CSAC*	*ED/GDPR*	*BCFI*
OECD.1	CSAC.4 CSAC.3	ED.5 ED.4 GDPR.1	BCFI.1
OECD.2	CSAC.6	ED.5	
OECD.3	CSAC.2	ED.3	BCFI.3
OECD.4	CSAC.5	ED.5 ED.3	
OECD.5	CSAC.7	ED.7 GDPR.6	BCFI.4
OECD.6	CSAC.8	ED.2 GDPR.2	BCFI.2
OECD.7	CSAC.9	ED.6	
OECD.8	CSAC.1 CSAC.10	ED.8 ED.1 ED.9	
		GDPR.3	BCFI.7
		GDPR.4	
		GDPR.5	
			BCFI.5
			BCFI.6

VII. CONCLUSION

Privacy regulations are growing in relevance and dictates how organizations and enterprises may collect, use, disclose, retain, and destruct personal information. Nowadays, it is representative of the principles behind privacy legislation in many nations and is used as the privacy standard basis for practical application in various specific contexts of data protection.

In the comparison we conclude that these privacy standards have similar principles, even though they may differ in the terminology and on how the overlapping concepts are divided. In general, the structure of these privacy standards address the way in which organisations satisfy contractual obligations and determine how data should be collect, use, and disclosed. This comparison benefits security and privacy

professionals since the results can be used to ensure that their organization's practices are consistent with countries in which they may exchange information.

REFERENCES

[1] Brasil. Marco Civil da Internet. Lei 12.964/14. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm>. Acesso em: 10 jun. 2018

[2] Brendan Van Alsenoy. Allocating responsibility among controllers, processors, and "everything in between": the definition of actors and roles in directive 95/46/ec. Computer Law & Security Review, 28(1):25 – 43, 2012.

[3] Decreto Legislativo. Codice in materia di protezione dei dati personali. In Gazzetta Ufficiale, june 2003.

[4] Enrico Nardelli. Certification and Security in E-Services from E-Government to E-Business. Kluwer, 2003.

[5] Guidelines on the protection of privacy and transborder flows of personal data. Technical report, OECD, September 1980.

[6] Luiz Costa and Yves Poullet. Privacy and the regulation of 2012. Computer Law & Security Review, 28(3):254 – 262, 2012.

[7] Model code for the protection of personal information. CSA CAN/CSAQ830- 96, Canadian Standards Association, march 1996.

[8] Office of the Data Protection Commissioner. Data protection act. October 1998.

[9] République française. Loi numéro 78-17 du 6 janvier 1978 relative `a l'informatique, aux fichiers et aux libertés. In European Union, editor, Journal Officiel de la République Française, Janvier 1978.

[10] The OECD Privacy Framework. Technical Report C(2013)79, OECD, July 2013.

[11] The European Parliament and the Council. Directive 1995/46/EC of the European parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In European Union, editor, Official Journal of the European Communities, October 1995.

[12] The European Parliament and the Council. Draft version-regulation of the european parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (general data protection regulation). In European Union, editor, Official Journal of the European Communities, October 2013.

[13] United Nations General Assembly. Universal declaration of human rights(udhr), december 1948.

[14] WBP Raamwerk J.P. Leerentveld, G. W. van Blarkom. Wbp raamwerk privacy audit. Technical report, The Hague, 2000