Public Governance, Administration and Finances Law Review Vol. 4. No. 2. (2019) • 30–51.

Information Security Awareness in Public Administrations at an International Level[1]

Lilla Garayová*

* Lilla Garayová, JUDr., PhD., Paneuropean University in Bratislava, Faculty of Law, Institute of International and European Law. (e-mail: garay.lilla@gmail.com)

Abstract: Privacy and data protection laws have changed significantly over the last two decades. The highly networked and interconnected world we live in today was only a flash on the horizon in the 1990s. The Internet itself was still a whole new innovation for many people. Many businesses have not had a public website yet. Concepts, such as online social media platforms, did not exist – and certainly no one thought about how they should be regulated. Smartphones, wearable technology and artificial intelligence have made huge leaps over the past 20 years – powered by new ways of data acquisition and processing. As a result, courts and regulators have increasingly had to adapt the aging data protection laws to suit a constantly changing world for which they were simply not designed. Government digital agendas worldwide go hand in hand with this fast-paced digital evolution. Information security and awareness should be a crucial part of public administration agendas with the primary goal to protect information of all types and origins.

Keywords: public administration; privacy; data protection; private information

1. Introduction

In the global information economy, personal data has become the driving force of most of today's online activity. Every day, a great deal of information is transmitted, stored and collected worldwide, allowing a tremendous improvement in computing and communication power. In developing countries, online social, economic and financial activities have been facilitated through the use of mobile phones and improved internet connectivity. As more economic and social activities move online, the importance of data protection and privacy is increasingly recognised, not only in the context of international trade. At the same time, the current data protection system is very fragmented and has different global, regional and national regulatory approaches.

In this study we will provide a comprehensive overview of the current situation and an analysis of the development trends of compatibility of data protection policies at international level. We also aim to provide a new and balanced view of privileged data protection issues by considering the views of different stakeholders. The conclusions of this study should contribute to reflection on how to increase international compatibility in data protection and privacy, in particular in relation to public law as well as international trade

and provide *de lege ferenda* proposals that could serve as inspiration for countries planning to introduce new laws or amendments to existing laws.

The protection of personal data belongs to the area of fundamental human rights and freedoms. Personal data is sensitive information that serves to identify a person and can only be processed with his or her consent. Everyone has the right to protection from unauthorised interference in private and family life, as well as protection against unauthorised collection, disclosure or other misuse of personal data. The processing of personal data should be designed to serve humanity. The right to the protection of personal data is not an absolute right; it must be assessed in relation to its function in society and must be balanced with other fundamental rights, in accordance with the principle of proportionality.[2] Rapid technological development and globalisation have brought new challenges in the area of personal data protection. The extent of collection and sharing of personal data has increased considerably. Technology enables private companies and public authorities to use personal data to an unprecedented extent in carrying out their activities. Natural persons are increasingly disclosing their personal data, including on a global scale. Technology has transformed both economic and social life and should further facilitate the free flow of personal data on a global scale and transfer to third countries and international organisations, while guaranteeing a high level of protection of personal data. The economic and social integration resulting from the functioning of the internal market has led to a significant increase in cross-border flows of personal data.

Data protection is directly related to trade in goods and services in the digital economy. Insufficient protection can create negative effects on the market by diminishing consumer confidence, and too strict protection can unduly restrict businesses, resulting in adverse economic effects. Ensuring that laws take into account the global nature and scope of their application and promote compatibility with other frameworks is essential for global trade flows that increasingly rely on the Internet. Many social and cultural standards around the world include respect for privacy. While the basic privacy policies contain many common features across countries, interpretations and applications vary considerably in specific jurisdictions. Some protect privacy as a fundamental right, while others base individual privacy on other constitutional doctrines or delicts. Others still have to accept privacy. Such differences will increasingly affect individuals, businesses and international trade. Internationally compatible data protection regimes are desirable as a way of creating an environment that is more predictable for all stakeholders involved in the information economy and building trust online. New technological developments increase this need. Data protection legislation must carefully address the changing needs and opportunities associated with these changes in order to facilitate potential benefits.

In order to ensure a consistent level of protection of personal data and to avoid differences between the jurisdictions of different States that could hinder the free movement of personal data, it is necessary to adopt rules providing legal certainty and transparency for economic operators, including micro, small and medium-sized enterprises, and providing individuals in all countries of the world with the same level of legal enforceable rights, ensuring consistent monitoring of the processing of personal data and providing for equivalent sanctions, as well as effective cooperation between the supervisory authorities of

the countries of the world. The proper functioning of the international market requires that the free movement of personal data is not restricted or prohibited for reasons connected with the protection of individuals in the processing of personal data. In order to avoid a serious risk of circumvention, the protection of individuals should be technologically neutral and not dependent on the technological solutions used. The protection of individuals should apply to the processing of personal data by automated means, as well as to manual processing if personal data are stored in or to be stored in the information system.

Efforts to achieve balanced, flexible and compatible data protection regulation have become an urgent global objective. Some countries have strong regulatory mechanisms, while others have outdated legislation or none at all. In order to achieve adequate protection that enables innovation and facilitates trade, it is essential to continue the national, regional and global dialogue of all stakeholders.

2. Key Privacy Concerns in an International Context

Data and privacy concerns are manifested in many different dimensions. Governments – especially those in developing countries that are trying to adopt data protection legislation – have difficulties in modelling their data protection regimes, although most have opted for an approach in line with EU legislation.

Common challenges include:

1. the time needed to adopt legislation
2. the financial costs of implementing and enforcing the data protection regime, and
3. lack of public and private sector knowledge and cooperation between governmental entities regulating in parallel

In some countries, lack of understanding and fear in society can aggravate one or more of the above concerns. Concerned consumers, concerns about the integrity of payment systems, hidden costs, fear of fraud and product quality are often more pronounced in the context of international e-commerce. Building trust in the online environment is crucial, and confidence is reflected in transactions with government and private actors. Studies show that citizens are concerned about how their personal data are collected and used and they also point out that these concerns are growing.[3] The lack of clarity in terms of protection and remedies tends to aggravate these concerns.

The most commonly highlighted concerns are:

1. Too strict protection regimes will disproportionately restrict activities, increase the administrative burden and hamper innovation.
2. Uncertainty and compatibility between schemes increase uncertainty with negative effects on investment.
3. Given the link between cross-border e-commerce and data protection, different regimes will prevent the uptake and dissemination of emerging technological developments, thereby reducing potentially accompanying societal benefits.

Although there are significant differences in data protection laws in different countries around the world, there is a more universal consensus on the fundamental principles of personal data protection, which are considered to be at the core of most national legislation and international regimes. This set of basic principles can serve as a useful starting point for efforts to achieve greater compatibility and harmonisation on a global scale. There is currently no uniform agreed model of data protection legislation. However, compatibility is an established objective of many global and regional initiatives in the area of personal data protection. There are a number of challenges in the development and implementation of data protection legislation. We believe that areas where action is particularly needed are:

- addressing gaps in the legal protection of personal data
- addressing new technologies
- management of cross-border data transfers
- strengthening the enforcement of justice
- determination of authority in the field of personal data protection

The number of national data protection laws has risen sharply in the last decade, but large gaps remain in the legislation of the different countries. Some countries have no legislation in this area, others have partial laws and some laws that are outdated and require amendments. In this study, we would like to provide considerations *de lege ferenda* that can help countries that are developing, revising or amending and supplementing their data protection laws.

For countries that still do not have the relevant legislation, governments should develop laws that should apply to data processed by government and the private sector and remove the exemptions to achieve greater coverage of personal data protection. The core set of principles is found in the vast majority of national data protection legislation as well as in global and regional initiatives. Adopting this core set of policies enhances international compatibility while allowing some flexibility for domestic implementation.

The creation of a single central regulatory authority shall be encouraged, where possible, with a combination of supervisory and complaint functions and powers. In addition, the trend is to extend enforcement powers as well as to increase the extent and scope of fiscal constraints and data protection sanctions. It is critical to address cross-border data transmission issues with specific text and to support one or more mechanisms that businesses can use to facilitate international data flows.

In an increasingly globalised economy, where more and more economic activities are carried out online, it is impossible to remain silent on this issue. A modern approach to addressing this seems to be allowing companies to consider a range of options. National data protection legislation should avoid (or remove) clear barriers to trade and innovation. This may include avoiding or removing data localisation requirements that go beyond the basic options for managing cross-border data transfers. A useful test that has emerged in this area is the requirement that such provisions should not be "disguised restrictions on trade".

It is also increasingly difficult to ignore the need to balance personal data protection and state surveillance requirements. In general, countries should implement measures that set appropriate monitoring limits and conditions.

In order to promote the international compatibility of different legislations, it is important to avoid duplication and fragmentation of regional and international approaches to the protection of personal data. It would be preferable for global and regional organisations to focus on a single consolidating initiative or a smaller number of initiatives that are internationally compatible rather than carrying out multiple initiatives. Where possible, similarities to the basic principles should be used to establish mechanisms for recognition and compatibility between different legal frameworks. Future work to achieve greater compatibility will require the effective involvement of all stakeholders, including the government, the private sector and civil society representatives. Their involvement must go beyond general discussions in order to be formally involved in the process of developing the legal framework. This active involvement will also help to develop measures that promote a higher level of legal certainty and trust among stakeholders, which will increase the overall effectiveness of the legal frameworks.

Most regional and global initiatives do not mention the issue of monitoring initiated by governments. However, we believe that it is essential that national legislation and global and regional initiatives recognise the existence of surveillance issues and try to address them directly. While monitoring issues often have an international or cross-border dimension, the extraterritorial nature of data flows must be addressed separately, as they relate to state sovereignty. The UN Declaration on Digital Rights can serve as a platform to consider the link between data protection and surveillance.[4] The development and promotion of international and regional data protection initiatives should also take into account the compliance burden and the potential for adverse effects on trade, innovation and competition.

Finally, favouring provisions that build consumer confidence in regulatory models will help to expand e-commerce. The most important is the development of effective policies around the world, especially with the advent of the latest technological advances. Countries should endeavour to counterbalance the various legitimate concerns of data protection stakeholders, while cautiously avoiding solutions that unduly restrict trade. Rebalancing can have serious consequences for the protection of fundamental rights as well as for international trade and development.

Efforts for a balanced, flexible and compatible legal regulation of personal data protection have become an urgent goal worldwide. Some countries have strong regulatory mechanisms, while others have outdated legislation or none at all. In order to achieve adequate protection that enables innovation and facilitates trade, it is essential to pursue a multi-stakeholder national, regional and global dialogue.

3. Increasing Importance of Personal Data Protection

Data protection laws date back to the 1970s, reflecting concerns about the development of computer and communication technologies and their ability to remotely process large volumes of data. In the global information economy, personal data has become the driving force of most of today's online activity.

Every day, a huge amount of information is transmitted, stored and collected around the world as a result of the huge improvement in computing and communication power. In developing countries, online social, economic and financial activities have been facilitated through mobile phones and better internet access. The cross-border nature of the Internet, as well as the speed and volume of communications itself, cause cyber security problems, such as those related to the identification, investigation, jurisdiction, criminalisation and prosecution of those who commit security and privacy violations. In this environment, information security is a problem for governments, businesses and consumers. Protecting data and privacy rights online is a major and increasingly pressing challenge for policy makers. The scrutiny of and access to information obtained through online activities concerns legislators whose task is to protect their citizens from unauthorised interference and harm.

From a commercial point of view, the transmission of data to and from developing countries may be hampered by the lack of domestic legal protection, which may result in missed business opportunities. Adequate legal instruments to ensure data protection and privacy are still lacking in most developing countries. The scope of the definition of personal data varies (wide or narrow) depending on the jurisdiction, and privacy laws vary considerably between countries and regions.

While many national, regional and international initiatives have pursued distinctly different regulatory approaches, there is a considerable degree of harmonisation of the underlying principles that underpin them. The common principles include the need to have a legitimate reason for any processing activity obtained either by consent or by some other justification. Obligations regarding the quality of the processed personal data are another fundamental principle that requires data to be accurate, complete and updated. Compliance with this principle should be mutually beneficial to both the processing entity and the processor. The role of data security is essential. Whether physical, logical or organisational, security measures should protect against intentional misuse as well as accidental loss or destruction of data. As with data quality issues, the needs of the individual data subjects and the data processing entity – and in principle society as a whole – should be combined in implementing adequate data security. Although there is a broad agreement on fundamental principles, there is no consensus on how best to apply them.

Some data protection regimes apply equally to everyone who processes personal data. Other regimes apply different rules to specific sectors (e.g. health, education), types of processing entities (e.g. public authorities) or data categories (e.g. children's data). In such jurisdictions, some sectors are not subject to regulatory controls at all. A distinction may also be made between regimes which operate primarily through enforcement actions brought by individuals or their representative groups and regimes that confer enforcement powers on a specialised supervisory authority, which continuously monitors the behaviour of those processing personal data. Some modes work by combining both approaches. Data protection is seen as an important area of law, policy development and regulation. It combines elements of human rights and consumer protection, and in many international agreements and individual jurisdictions, the protection of personal data is even considered a fundamental right. At the same time, many stakeholders see data protection regulation

as a legal framework that facilitates the development of new technologies and innovations and promotes international trade and development. Data protection regulation is currently a very topical issue, as evidenced by a number of recent events:

- In 2015, the United Nations appointed a Special Rapporteur on the right to privacy.
- The European Union has adopted a new general data protection regulation, Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This Regulation is an essential step towards strengthening the fundamental rights of citizens of the digital age and facilitating entrepreneurship by simplifying the rules for companies in the digital single market. At the same time, the unified legislation will put an end to the current fragmentation and costly administrative burden.
- Data protection has been included in several international trade agreements.
- Data protection regulation has been considered in several lawsuits with a high degree of professionalism on national surveillance issues.
- Many countries are drafting new data protection laws or reviewing existing legislation.
- The European Union and the United States have renegotiated a long-term cross-border data protection agreement (the former EU–U.S. Safe Harbor framework, now called Privacy Shield), one of the few alternatives for transmission of data outside the EU and therefore its existence is very important.
- Several global and regional organisations have issued (or are preparing) multilateral agreements and/or guidelines on the protection of personal data.

4. Key Challenges in Drafting Data Protection Laws

While many of the global and regional initiatives discussed in this publication are aimed at increasing interoperability between personal data protection regimes, the key problem is that huge gaps remain in the scope of data protection legislation. These gaps fall into three main categories:

1. Countries without personal data protection legislation

The number of countries with data protection legislation has risen sharply in recent years, currently reaching a total of 107 countries that have comprehensive data protection laws, or at least partial data protection legislation. However, this still leaves almost 30% of countries in the world without applicable privacy laws.[5] Personal data in these countries receive a low level of protection, thus reducing legal certainty and confidence in a wide range of business activities. These countries may also be cut off from international business opportunities, as many business transactions require cross-border data transmission, subject to minimum legal requirements. These requirements are difficult (but not always impossible) to meet in the absence of basic data protection legislation. At least 35 countries are currently drafting data protection laws to address this gap. However, the development and

implementation of data protection laws is a time-consuming and complicated process. The United Nations surveys of government officials in 48 African, Asian and Latin American and Caribbean countries highlight the need for awareness-raising and knowledge among lawmakers and courts in order to formulate and effectively enforce informed data protection policies and laws.

2. Countries with legislation containing large gaps and exemptions

Many national data protection laws contain significant gaps and exemptions. For example, some laws exclude small businesses (such as Australia and Canada) or small data sets (such as Japan excludes data sets with less than 5,000 records) from the privacy laws. Other exceptions in some laws apply to:

- types of data subjects (e.g. only children's data and no employee data)
- data sensitivity (e.g. only to sensitive data such as health or financial records)
- data sources (e.g. limited to online or offline data collection)
- sectoral data (e.g. private and public sector exceptions or laws that are limited to specific sectors such as health and credit)

The exceptions are so numerous and so complex that the entire textbook could only be written with a list of exceptions and loopholes in the privacy laws. These exceptions are generally common in North America, Asia and the Pacific, but less typical in Europe, South America and Africa, where data protection legislation tends to provide comprehensive coverage. Exceptions create several legal problems. They require a wide range of stakeholders (business partners, consumers and regulators) to comprehensively identify and categorise data. They severely limit countries' ability to meet the "adequacy test" for cross-border credit transfers and can also lead to complex complaints and disputes.

3. Countries where companies are allowed to exclude certain services or practices from the scope

The third type of gap is less common but has been steadily growing in recent years. Some national laws and regional initiatives allow individual companies to determine the "scope" of the data protection they offer to consumers. There are two ways to do this:

First, a company can join a data protection regime (for example, the EU–U.S. Safe Harbor framework/EU–U.S. Privacy Shield or cross-border privacy rules), but their membership is limited to specific activities. The scope is usually published in the online register. Typical limitations restrict coverage to online or offline data collection, consumer or employee data, or other general categories. However, some scope constraints exclude whole countries from the protection offered by large multinationals.

Second, a company may exclude certain activities from protection by including exceptions in its privacy policy. Organisations are increasingly excluding specific services such as mobile apps, cloud services and software. These exclusions often apply to dispute resolution

when a company uses a third-party dispute resolution provider, so these exclusions can be quite significant for consumers. In practice, the second type of exclusion may not be entirely legitimate if a complaint is lodged with the regulator concerned. Regulators have a wide range of powers in this area. In the United States of America, the Federal Trade Commission (FTC) may take steps for "unfair" behaviour, which may limit the use of such exceptions. Such specific exclusions are a relatively new phenomenon in international data protection regulation and their state (and future) is uncertain. Overall, however, it is difficult to promote global interoperability, while these three types of "gaps" in coverage remain.

5. Cross-border Data Transfers

Overall, it is generally recognised that there should be legislation on cross-border data transfers, but there is a wide range of approaches to this issue and there is no single global model to manage it yet. At a national level, some countries have no restrictions on the transfer of personal data to foreign jurisdictions (such as the United States of America). Most countries have some restrictions in place, usually accompanied by a long list of exceptions. Typical exceptions fall into two broad categories.

1. One-off exceptions – On a global scale, there seems to be a broad consensus on one-off "exceptional circumstances" that allow cross-border data transmission. A recent report by the International Center for Policy Management states that the following exceptions have already become common:[6]

a) the transfer is necessary for the performance of the contract between the data subject and the operator or between the operator and the third party and is concluded at the request of the data subject; or is in the interest of the data subject
b) transmission for the purposes of legal proceedings or for the purpose of obtaining legal advice or for the establishment, exercise or protection of legal rights
c) the transfer is necessary to protect the vital interests of the data subject

2. Ongoing exceptions – The use of ongoing exceptions is less consistent. The following list demonstrates the wide range of approaches available, but there is no consistency or global consensus in their use.

a) The "reasonableness" approach (sometimes known as the white list) assesses whether the entire jurisdiction of destination provides a sufficient level of protection for the transfer of personal data. This approach is used by different countries, including members of the European Union, Israel, Japan and Switzerland.
b) The "binding rules" approach assesses whether a particular company has put in place processes and independent control mechanisms that provide a sufficient degree of protection for the transfer of personal data (usually across a group of companies). This approach is used in a system of binding EU business rules. Some individual jurisdictions also have the potential to recognise these types of binding rules, notably Australia and Japan.

c) The "model contracts" approach assesses whether the specific wording in the contracts provides a sufficient degree of protection for the transfer of personal data. So far, this approach has only been used in the EU.
d) The "consent" approach examines whether individual consumers can agree to transfer their data abroad. This approach is used in the EU and some other jurisdictions but is subject to additional conditions regarding the nature of consent. Consent may be difficult to prove and does not constitute an effective guarantee of protection.

Not surprisingly, many countries have decided to adopt a combination of several approaches to managing cross-border data transfers, as there is no single mechanism that stands out as completely positive. As a result, the law on cross-border data transfers is fragmented and inconsistent.

The problems associated with cross-border data transfer are to some extent addressed through international trade agreements. One recent example of the agreement is the Trans Pacific Partnership Agreement (TPP), which covers 12 countries. TPP addresses the issue of balancing data protection with special regard to trade. In particular, it imposes restrictions on the scope of the Data Protection Regulation which signatories may lay down in their national legislation and is partly based on Article XIV of the WTO General Agreement on Trade in Services. Article XIV allows for restrictions on cross-border transfers if they meet four requirements:

1. the law must "achieve a legitimate public policy objective" – this seems to be a very direct requirement
2. the law must not be "applied in a manner which would constitute a means of arbitrary or unjustified discrimination"
3. the law must not be a "disguised restriction on trade"
4. the law must not "impose restrictions on the transmission of information beyond what is necessary to achieve the objective"[7]

It seems that this four-part test could provide a potential basis for a global standard to determine whether a restriction went "too far". These criteria have a good chance of removing "hidden trade restrictions" and have the potential to increase interoperability and harmonisation beyond the signatories to the agreement.

Overall, the possibilities for managing cross-border data transfers are diverse and varied. Most countries adopt a combination of the above measures and give businesses considerable leeway in managing their own cross-border transfers. This is largely due to the recognition of the reality of modern data-processing systems as well as the current volumes of cross-border transfers that occur at any given moment.

6. Strengthening Powers and Determining Jurisdiction

Currently, we can see a trend towards strengthening enforcement and sanctioning powers in the area of personal data protection. This is a response to a number of high-profile cases

where existing regulatory powers have proven to be disproportionate in view of the widespread impact and scale of privacy breaches. Strengthening enforcement has been a major issue in amending and updating laws (especially in Australia, the EU, China and Japan). The United States is considered a leader in this area. Although there are many loopholes and inconsistencies in the U.S. legislation, the country has had good experience of using extensive sanctions to prevent neglect of privacy. The imposition of large sanctions is considered important for:

- the target company (as a clear signal to senior management and employees to reform their practices)
- the consumers concerned (as a form of compensation for the damage they have suffered), and
- also as a wider deterrent to the whole industry

Jurisdiction is an extremely important issue in all areas of law, in particular in the areas of cybercrime, tax law and intellectual property law. Data protection regulation has become a very important issue, partly because of the extensive flow of data across borders, partly because of the lack of a single global data protection agreement (and the consequent fragmentation of regulation). In the absence of an international agreement, determining jurisdiction is very difficult.

The issue of determining jurisdiction has long been a source of debate and legal reform. The U.S. Child Online Privacy Protection Act (COPPA) extends to foreign service providers who direct their activities to U.S. children or consciously collect information from U.S. children. A recent law reform in Japan resulted in a new request (which came into force in 2017) stating that if a data controller outside Japan collects personal information concerning Japanese citizens, then that foreign controller will be required to meet the requirements listed in the Japanese law.

Regulation (EU) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data contains an extraterritoriality clause (Article 3) stating:

1. This Regulation shall apply to the processing of personal data in the context of the activity of the controller or processor in the Union, whether or not processing is carried out in the Union.

2. This Regulation shall apply to the processing of personal data of data subjects who are situated in the Union by an operator or intermediary not established in the Union, the processing activities being related to:

a) the offering of goods or services to those data subjects in the Union, whether or not payment is made to the data subject, or
b) monitoring their behaviour within the Union[8]

These reforms are part of a trend towards national data protection regulations that seek to capture any activity that targets local people, regardless of the actual location of the company.

Privacy requirements may limit the possibilities for innovation or create an unrealistic burden on compliance businesses (especially for smaller businesses). Some examples of data protection requirements that have the potential to burden businesses are as follows:

1. Registration requirements

In a small number of jurisdictions (mostly in Europe), data controllers are required to register their operations and sometimes their individual datasets with the local data protection authority. This requirement relates to the historical introduction of data protection regimes at a time when data processing was considered a key risk to privacy. Over time, some data protection authorities considered the registration procedure to be a useful form of general regulation and supervision. In many developing countries, the registration process has also become an important source of revenue. In jurisdictions where data protection relies on membership of a specific system (such as the EU–U.S. Privacy Shield), membership in these systems requires a combination of payments to a central system operator (such as the U.S. Department of Commerce) plus payments to service providers dispute resolution (such as the American Arbitration Association) and payments for third-party certification services (such as TRUSTe). Most fees in these systems must be paid annually. For businesses, registration requirements can be a significant financial burden. Some processes are time-consuming and bureaucratic, and many require fees, whether one-time or annual. Registration requirements may also hamper the ability of businesses to create a single, comprehensive system of data protection processes that could be used in all jurisdictions.

2. Requirements for the appointment of Data Protection Officers

A common requirement in national legislation is that each undertaking appoints a specific Data Protection Officer (the specific name varies slightly in each national law). This does not represent a significant burden in most large organisations if such appointments are common, but it may be a burden for smaller businesses.

3. Requirements for the establishment of data centres

In a few rare cases, data protection laws require businesses to set up either data centres or offices at a specific location. These requirements are a significant obstacle for all businesses but are particularly challenging for smaller businesses and new entrants. Overall, they can effectively reduce opportunities for smaller, newer businesses and negatively affect interoperability. Smaller businesses play an important role in managing innovation and competition, yet they face difficulties in jurisdictions with high compliance burdens. However, the interests of businesses (including small ones) are not completely neglected in global, regional and national personal data protection initiatives. Most global and regional initiatives include a warning of linguistic complexity, excessive burdens on privacy requirements.

7. Global Developments and Trends in the Field of Personal Data Protection

Privacy is not the subject of a single comprehensive global agreement or contract. Rather, it is included in a number of international and regional instruments, each covering a particular group of countries. These global and regional initiatives differ in scope and application – many are simply voluntary guidelines. This chapter discusses major global initiatives, plus the strengths and constraints of each system. In short, we would like to focus on major initiatives with an almost global reach: the UN, the Council of Europe, the OECD and IDPC. Each of these initiatives has its strengths and weaknesses.

1. UN

The United Nations has long promoted the right to privacy through human rights treaties, in particular through Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights. In the period of 2013–2015, the UN strengthened its role in the field of privacy by means of two highly profiled measures. The first was the publication of the Digital Rights Declaration. The second was the appointment of a UN Special Rapporteur on the right to privacy.

Declaration on the right to privacy in the digital age – In December 2013, the UN General Assembly adopted Resolution 68/167,[9] expressing its deep concern about the negative impact that monitoring and interception of communications may have on human rights. The General Assembly confirmed that the rights held by citizens offline must also be protected online and urged all states to respect and protect the right to privacy in digital communications. The General Assembly also called on all States to review their procedures and legislation regarding communications monitoring, interception and collection of personal data and underlined the need for States to ensure the full and effective implementation of their obligations under international human rights law.[10]

The resolution notes that international human rights law provides a universal framework under which any interference in individual rights, including the right to privacy, must be assessed. The International Covenant on Civil and Political Rights, which has so far been ratified by 167 states, states that no one shall be subjected to arbitrary interference in private life, family, home or correspondence, nor to attacks on their honour and reputation.[11] It further states that everyone has the right to the protection of the law against such interference or attacks. Other international human rights instruments also contain similar provisions. Although the right to privacy under international human rights law is not absolute, any case of interference must be subject to a thorough and critical assessment of its necessity, legitimacy and proportionality. The resolution was followed by a detailed report published in 2014: Study by the High Commissioner for Human Rights on the right to privacy in the digital age (A/HRC/27/37).[12] The report concludes that practices in many countries have revealed a lack of adequate national legislation, weak procedural guarantees and ineffective supervision, which together contributed to a lack of responsibility for arbitrary or unlawful interference with the right to privacy.

UN Special Rapporteur on the Right to Privacy – The Special Rapporteur is an independent expert appointed by the UN Human Rights Council to examine and report on specific issues. In July 2015, the Human Rights Council appointed Professor Joseph Cannataci of Malta as the first ever UN Special Rapporteur on the right to privacy. Pursuant to Resolution 28/16 of the Human Rights Council, the Special Rapporteur shall:

a) collect relevant information, including information on international and national frameworks, national practices and experiences; study trends, developments and challenges regarding the right to privacy and make recommendations to ensure its support and protection, including in the context of challenges arising from new technologies
b) seek, receive and respond to information from States, the United Nations and its agencies, programs and funds, regional human rights mechanisms, national human rights institutions, civil society organisations, the private sector, including business entities
c) remove possible obstacles to the enforcement and protection of the right to privacy, identify, exchange and enforce principles and best practices at national, regional and international level and, in this context, submit proposals and recommendations to the Human Rights Council, including in the light of these facts and in particular to the particular challenges of the digital age
d) participate in and contribute to relevant international conferences and events in order to promote a systematic and coherent approach to mandate issues
e) raise awareness of the importance of promoting and protecting the right to privacy, addressing the specific challenges of the digital age as well as providing information to individuals whose privacy has been violated, ensuring access to effective remedies, in accordance with international human rights obligations
f) report on alleged violations of the right to privacy wherever they occur, as set out in Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights, including the challenges arising from new technologies, and alert the Council and the UN High Commissioner for Human Rights on situations of particular concern
g) submit an annual report to the Human Rights Council and the General Assembly

In March 2016, the UN Special Rapporteur prepared his first report on the right to privacy, which was presented to the Human Rights Council (A/HRC/31/64). The report describes his vision of the mandate and provides an overview of the state of privacy in early 2016 and a work plan for the first three years of the mandate. In order to facilitate the process of further elaborating the dimensions of the right to privacy and its relation to other human rights, the Special Rapporteur has developed a Framework Action Plan.

The strengths of UN initiatives include universal respect and global coverage, a long history of promoting and protecting human rights; and recognition of privacy as a fundamental right. One of the limitations of UN initiatives is, in particular, that the current provisions are too theoretical for day-to-day operations – the right to privacy must be translated into a detailed set of principles. Another problem is that the UN is facing some significant constraints in terms of resources, whether material or personnel.

2. The Council of Europe

The right to the protection of the private sphere of the individual from interference by other entities, in particular the State, was for the first time enshrined in Article 12 of the UN Universal Declaration of Human Rights in 1948 and referred to respect for private and family life. The Universal Declaration of Human Rights has influenced the development of other human rights instruments in Europe. The Council of Europe was established after World War II with the intention of bringing together European states in the promotion of the rule of law, democracy, human rights and social development. To this end, the Council of Europe approved the European Convention on Human Rights in 1950, which entered into force in 1953. Member States have an international obligation to comply with the ECHR provisions. All Member States of the Council of Europe have incorporated the ECHR into or have entered into force in their national legislation and must therefore comply with the provisions of this Convention.

The right to the protection of personal data forms part of the rights protected under Article 8 of the ECHR, which guarantees the right to respect for private and family life, dwelling and correspondence and lays down the conditions for the admissibility of restrictions on that right. In its case law, the ECHR has considered many data protection cases, including, inter alia, interception of communications,[13] various forms of surveillance[14] and protection against the retention of personal data by public authorities.[15] Article 8 of the ECHR not only requires States to refrain from taking any action that might undermine this right enshrined in the Convention, but in certain circumstances imposes a positive obligation to actively ensure effective respect for private and family life.

Council of Europe Convention No. 108 – The emergence of information technology in the 1960s has made it increasingly urgent to adopt detailed rules on the protection of individuals by protecting their personal data. In the mid-1970s, the Committee of Ministers of the Council of Europe adopted several resolutions on the protection of personal data referring to Article 8 of the ECHR. In 1981, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) was prepared for signature. Convention 108 was the only legally binding international data protection document. At present, Convention 108 is the most important binding international agreement on the protection of personal data. Although this Convention was established in the Council of Europe, its membership is open to each country, and several non-European countries have already signed the Convention.

All member states of the Council of Europe have ratified the Convention and implemented data protection laws that comply with the Convention (the last one was Turkey, where ratification took place in 2016). Uruguay was the first non-European country to become a Party to the Convention in 2013. Currently, the Convention has been ratified by 9 non-European countries (Argentina, Burkina Faso, Cape Verde, Mauritius, Morocco, Mexico, Senegal, Uruguay and Tunisia). The Convention differs from many other global initiatives in that it is binding on signatories. Data in the private and public sectors, such as the processing of personal data in the judiciary or law enforcement authorities, protects the individual from abuse that could accompany the collection and processing of personal data, while regulating the cross-border flow of personal data.

With regard to the collection and processing of personal data, the principles laid down in the Convention related in particular to fair and lawful collection and automated processing of data which are stored for specified legitimate purposes and are not used for purposes incompatible with those purposes or absolutely necessary. These principles also regulate the quality of the data, in particular its adequacy and relevance, as well as the fact that the data must not be redundant (proportionality) and must be accurate. In addition to providing safeguards for the collection and processing of personal data, the Convention regulates (where there are no adequate legal safeguards) the processing of so-called "personal data", i.e. sensitive data such as race, political attitudes, health, religious beliefs, sexual life, or criminal record data. The Convention also enshrines the right of an individual to know about the retention of data concerning him and to be able to correct such data as necessary. Restricting the rights set out in the Convention is only possible in cases of overriding interests, such as national security or defence.

Among the strengths of the Council of Europe Convention 108 include comprehensive coverage, the existence of broad acceptance of the principles contained in the Convention, the possibility of any country to join, cooperation under the open procedure. The great advantage is the binding nature of the agreement, which leads to effective harmonisation; and that the Convention has strong support of other initiatives (e.g. endorsed by the International Data Protection Commissioner as the best available global model). The limitations of the Council of Europe Convention include, in particular, its Eurocentric nature (although currently extending rapidly to non-European countries). Overall, Convention 108 is the most promising international development in an area where each initiative faces enormous challenges.

3. OECD

Member States of the Organization for Economic Co-operation and Development (OECD) have developed the OECD Guidelines on the protection of privacy and cross-border flows of personal data in consultation with a broad stakeholder group. With the introduction of information technology in various areas of economic and social life, and with the increasing importance and potential of automated data processing, the Organization for Economic Co-operation and Development decided in 1980 to issue guidance on international privacy policy and the cross-border flow of personal data. The rapid and ubiquitous development of information and communication technologies and infrastructures, characterised by a phenomenon such as the Internet, has accelerated developments towards a global information society. The OECD has therefore focused on how this guidance could best be applied in the 21st century to help ensure respect for privacy and the protection of electronically accessible personal data.

The guideline on privacy and the cross-border flow of personal data was adopted as a recommendation of the OECD Council in support of the three principles that are binding on OECD member states: open democracy, respect for human rights and the free market economy. It entered into force on 23 September 1980. The Privacy Guidelines

constitute an international consensus on the general approach to collecting and managing personal information.

The principles set out in the Privacy Guidelines are comprehensible, flexible to apply and formulated sufficiently broadly to be adapted to technological changes. The principles include all media for automated processing of individual data (from local computers to networks with complex national and international branches), all types of personal data processing (from human resources to compiling customer profiles) and all data categories (from transient data to fixed data, from the most mundane to the most sensitive). The principles are applicable both nationally and internationally. They have gradually been incorporated into a large number of national regulatory or self-regulatory instruments and are still frequently used in both the public and private sectors. The Guidelines can be governed by any country, not just OECD members.

The OECD itself has 34 members, of which 32 have already implemented comprehensive data protection laws prior to the adoption of the Guidelines. At the end of March 2016, the Turkish Parliament approved a draft data protection law aimed at aligning the Turkish regime with the EU regime, leaving the U.S. as the only exception (the U.S. is more likely to use the sectoral approach to data protection). However, the real impact of the OECD Guidelines is its impact on the content of privacy laws around the world – far beyond the OECD membership. The Guideline contains eight privacy principles, which are those contained in most national privacy laws.

The strengths of the OECD Guidelines on Privacy include a long and respected history, generally accepted basic principles, a focus on striking a balance between data flows and data protection; wide support for diverse groups. The limitations of the OECD Guidelines on privacy include the absence of the principle of proportionality (or minimisation of data), the non-binding nature of the guidelines and focus on developed countries (although in practice the basic principles are largely applicable).

4. Initiatives of the International Data Protection Commissioners

The latest data protection initiative, which has an almost global impact, is the work of international data protection authorities. Their main role is to regulate national data protection legislation, but since their work involves more international disputes, they have begun to engage in a global privacy debate. There are three main initiatives:

1. annual meeting and conference
2. a system of cooperation on international and cross-border complaints, and
3. a statement of global privacy principles

For our purposes, the third initiative is of the utmost importance. At their meeting in 2005, the International Data Protection Commissioners issued a statement entitled: *The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities* (also known as the Montreux Declaration).[16] The Declaration called for the development of an international data protection convention and is one of the most important efforts to harmonise data protection laws worldwide. In particular, the Declaration states: Data

Protection and Privacy Commissioners express their desire to strengthen the international recognition of the universal nature of these principles. They agree to cooperate, in particular, with governments by international and transnational organisations in drawing up a universal convention on the protection of individuals with regard to the processing of personal data. To this end, the Commissioners called for:

a) the UN to develop a legally binding instrument that clearly lays down detailed data protection and privacy rights
b) any government in the world to promote the adoption of legal instruments for data protection and privacy in accordance with the fundamental principles of data protection and to extend them to its mutual relations, and
c) the Council of Europe, in accordance with Article 23 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), invites non-member States of the Council of Europe which already have data protection enshrined in domestic law to accede to

The strengths of the International Data Protection Commissioners' initiatives include significant global impact, real world experience, insight into current issues and emphasis on the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) as a global platform (instead of proposing something brand new). Restrictions on the initiatives of the Commissioners for International Data Protection include the lack of formal structure or follow-up and the non-binding nature of the declaration.

8. Conclusion

On the previous pages, we aimed to emphasise the importance of data protection management in the context of international trade and in the context of different global, regional and national approaches to data protection regulation. We recognise that there are various legitimate concerns regarding data protection and privacy – from consumers (civil society), businesses and governments. The challenge for data protection and privacy laws is therefore to balance these various concerns and interests, ideally in a way that does not unnecessarily restrict trade and innovation.

It is also essential to find solutions that are internationally compatible to facilitate cross-border online trade. As we have mentioned in this study, the current system is not satisfactory and, given the growing economic and social activity on the Internet and the introduction of new technologies, there is an urgent need to address the situation. Against this background, we evaluated the current situation and tried to find possible paths towards a system that provides an appropriate balance between data protection and data streams.

Key conclusions are: There is a recognised set of basic data protection principles. With a remarkable degree of harmonisation and coherence around the core principles of data protection in key international and regional agreements and guidelines, different implementation procedures exist. Although there are significant differences in the details

of data protection laws around the world, we can find greater agreement at the core of most national laws and international regimes.

These common basic principles are: openness, limitation of data collection, purpose specification, limitation of use, security data quality, transparency and accountability. This set of basic principles is a useful starting point for efforts for interoperability and legislative harmonisation. Countries that have not yet introduced laws, or countries that are updating or reforming their laws, should seek to incorporate these basic principles into their new (or amended) legislation. While the coherence of the principles may not guarantee full mutual recognition, it can significantly contribute to the compatibility of different policies.

In some other legal areas, international and regional organisations have come together to support a single initiative to achieve compatibility and harmonisation. For example, in the case of cybercrime, there is broad support for the development and extension of the 2001 Council of Europe Convention on Cybercrime, which now has 54 signatories, including many European countries, Australia, Canada, Japan and the USA. The Convention has led to the harmonisation of cybercrime legislation in many other countries, beyond the signatory members, as the basic provisions are often reflected in the national legislation of several States. On the contrary, there is no single global agreement on data protection. There are many regional and international initiatives in this area, some of which are in competition with each other. Although there are different approaches, there are quite a number of common views on the basic principles and broad agreement on the issues to be addressed. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe Convention No 108) is the agreement with the widest support and greatest potential for compatibility. The Convention may be signed by any country; already has a large number of supporters; it is based on generally agreed principles; has the support of key stakeholders (in particular civil society and regulators); and its binding nature would increase compatibility and interoperability. However, the Convention must attract key support in North America and Asia and the Pacific.

Regardless of which instrument will form the basis of cohesion, convergence of regimes may already occur. One example is the European Union. The European Union intends to make progress not only towards internal but also external cooperation: the EU is actively engaged in international data protection cooperation through various international fora, including the OECD and the Council of Europe (and intends to become a party to the revised Council of Europe Convention on Data Protection 108). The EU participates in a dialogue on privacy and data protection with regional organisations, in particular APEC.

Achieving the wrong balance between data protection and data flows can have serious consequences for the protection of fundamental rights as well as for international trade and development. In most cases, data protection initiatives have been developed in an open and transparent way, with opportunities for entry from different stakeholders' perspectives. For example, the Council of Europe Convention 108 contains a forum where all Member State governments, regulators, private sector stakeholders and civil society representatives can gather information and share information on the promotion and improvement of the

Convention. However, there are examples of initiatives that were developed without the opinion of external stakeholders. For example, international trade agreements are often considered to be developed through clandestine negotiations, which clearly limit the opportunities to hear the voice of the consumer – civil society.

Another key point for countries without a legal framework in the field of personal data protection is the establishment of an effective regulatory structure. The benefits of a single central regulator, in particular for international trade opportunities and for consumers in general, are considerable. While there are differences in the regulatory structure of the legislation, the creation of a single central regulatory authority seems to be strongly encouraged, where possible. Several countries have moved from a complex regulatory structure of several agencies to a simpler structure of national agencies (e.g. Japan has moved from 30 regulators to one central regulator). This is not always possible due to the federal nature of jurisdiction (e.g. Canada, Germany and India). However, the benefits of a single regulator, especially as regards international trade opportunities, are huge. Foreign companies then have to deal with only one focal point and a single regulator can achieve consistency by issuing a single set of guidelines or standards. Consumers will also be made much easier to deal with complaints and questions if there is a single regulatory body and at the same time, a single consistent set of decisions of the national regulatory authority will have a greater impact than a diverse set of decisions from several regulatory authorities. It is important that the regulator also has the role of complaint manager. Most regulators combine a general supervisory function with this specific task, with some exceptions. For example, the FTC in the United States of America is a strategic regulator (it may not respond to individual complaints), while dispute resolution in the United States is partly governed by private litigation and third-party providers. The Republic of Korea has formally divided the regulatory and complaints agenda between the two agencies.

Developing and implementing data protection laws is a complex and costly process that often requires a careful balance between data protection and data flows. Redressing the balance can have serious consequences for the protection of fundamental rights or for international trade and development. Future efforts to achieve greater compatibility will require the effective involvement of all stakeholders, including representatives of the private sector and civil society. This involvement must go beyond general discussions (conferences, seminars, etc.) to engage in the formal policy development process. Developing global and regional data protection initiatives also requires the involvement of developing countries in the debate. Too often, the debate is dominated by the interests of developed countries. Developed countries have the most advanced data protection laws and have the most experience in enforcing them but improving cooperation with developing countries is increasingly encouraged. The world is at the forefront of a transformational technological revolution, fuelled by the economic and social benefits of access to data. Emerging markets are competing with time to capture these benefits but are left out of the innovation dialogue that largely takes place among developed markets.

Global privacy laws are at a crossroads. So far, these laws have mostly focused on the rights of individuals. In general, the aim was to ensure the protection of individuals' private lives and to prevent their governments and businesses from being unfairly violated. However, interesting new pages are emerging in discussions on the future direction of

policy in this area. On the one hand, there is strong business pressure to allow a free flow of data, which is an essential part of a world in which economic growth is increasingly digital. On the other hand, individuals generally do not like the feeling that they are being spied on or that their data is beyond their control. The overall approach to this issue in the EU and some other jurisdictions is currently being resolved for the foreseeable future, but legislators in jurisdictions in which privacy is emerging are facing challenges.

The main question is where there should be the right balance between the right to privacy and the ability of companies to monetise individual data. On the one hand, there is an indication that the right to privacy is absolute and inviolable (in fact, it is referred to as a fundamental right in the EU). The supporters of this view consider that the right to the privacy of the individual is paramount – and it is not difficult to understand why this argument is attractive. Major privacy breaches and security failures are getting headlines with alarming regularity and show that many businesses are not investing as much in digital security as they should. In fact, even if proper and responsible investments have been made, it is often impossible for any company to ensure that no third-party attacker gets well into its systems.

Efforts to achieve balanced, flexible and compatible data protection regulation have become an urgent global objective. Some countries have strong regulatory mechanisms, while others have outdated legislation or none at all. In order to achieve adequate protection that enables innovation and facilitates trade, it is essential to continue the national, regional and global dialogue of all stakeholders.

The need for new legislation is fast approaching due to the unstoppable technological revolution. New technologies, including machine learning, artificial intelligence and fintech, offer countless benefits in terms of data analysis and quick and accurate decision-making in tasks that can take a lot longer. However, the testing and development of these technologies often relies on access to large data sets to achieve meaningful results.

Developers are faced with difficult decisions to move their operations to jurisdictions that place less restrictions on data handling for testing purposes. Once the products are functional, many companies find that if they choose to offer their services in jurisdictions with very strict privacy laws, they have to face a high regulatory barrier.

Some companies have taken the view that the costs of meeting these strict privacy obligations are too high to be justified until the product is well established. As a result, users in jurisdictions with strict privacy laws are increasingly finding that the latest technologies are not available in those jurisdictions. It is therefore important that all jurisdictions ensure the implementation of data protection laws in a way that does not hinder creativity and technological development. If they fail to do so, they risk their citizens becoming second-class passengers on the digital journey.

References

1 This work was supported by the Slovak Research and Development Agency under the contract No. APVV-16-0521.
2 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).
3 Data protection regulations and international data flows; United Nations Publication; UNCTAD/WEB/DTL/STICT/2016/1/iPub United Nations, 2016 Switzerland.
4 *The Age of Digital Interdependence,* Report of the UN Secretary-General's High-level Panel on Digital Cooperation, www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf (accessed 11 August 2019).
5 *Summary of Adoption of E-Commerce Legislation Worldwide,* Global Cyberlaw Tracker, http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx (accessed 11 August 2019).
6 Centre for Information Policy Leadership (CIPL), Cross-Border Transfer Mechanisms, www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_indonesia_ministry_of_comm_and_it_draft_regulation_august_20_2015.pdf (accessed 08 November 2019).
7 WTO General Agreement on Trade in Services, www.wto.org/english/tratop_e/serv_e/gatsintr_e.htm (accessed 08 November 2019).
8 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).
9 The right to privacy in the digital age: resolution / adopted by the General Assembly, A/RES/68/167, https://digitallibrary.un.org/record/764407/?ln=en (accessed 08 November 2019).
10 United Nations, Resolution adopted by the General Assembly on 18 December 2013, 68/167. The right to privacy in the digital age, www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167 (accessed 08 November 2019).
11 *The International Covenant on Civil and Political Rights,* https://treaties.un.org/doc/publication/unts/volume%20999/volume-999-i-14668-english.pdf (accessed 08 November 2019).
12 United Nations High Commissioner for Human Rights, *The Right to Privacy in the Digital Age* (an Overview), www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx (accessed 08 November 2019).
13 Copland v. The United Kingdom European Court of Human Rights [2007] C/62617/00, European Court of Human Rights.
14 Klass and others v. Federal Republic of Germany, Judgment, Merits, App. no. 5029/71 (A/28), (1979-80) 2 EHRR 214, IHRL 19 (ECHR 1978).
15 S and Marper v. United Kingdom, ECHR [2007] EHCR 110, 30562/04.
16 The International Data Protection and Privacy Commissioners, Montreux Declaration – *The Protection of Personal Data and Privacy in a Globalised World: A Universal Right Respecting Diversities,* 2005, https://edps.europa.eu/sites/edp/files/publication/05-09-16_montreux_declaration_en.pdf (accessed 08 November 2019).