

A world map with a light blue background and dark blue landmasses. Numerous red dots are scattered across the map, primarily concentrated in Europe, North America, and South America, with a few dots in Africa, Asia, and Australia. The dots represent various global locations.

A general guide to GDPR and its impact within and outside the EU

**Do's and don'ts for every business that
deals with Data Privacy**

Table of contents

01

Introduction

02

GDPR

- 04 General situation
- 04 The impact outside of the EU / EEA
- 04 Controller and Processor
- 04 What is personal data?
- 04 What is processing?
- 04 GDPR focus
- 04 Consent vs. information
- 04 International transfers of data
- 05 GDPR breaches
- 05 GDPR application to non-EU processors and data controllers
- 05 Differences in ancillary legislation amongst EU countries

03

GDPR three years after its introduction

- 13 Landmark Cases/Fines and their takeaways

04

Data privacy legislations introduced in other jurisdictions

- 18 United Kingdom
- 20 Switzerland
- 21 India
- 22 Mainland China
- 23 Hong Kong
- 25 Dominican Republic
- 26 Mexico
- 27 United States of America
- 28 California

01 Introduction

The introduction of the General Data Protection Regulation in 2018 marked a significant milestone in the evolution of data protection law. In overhauling the 1995 Data Protection Directive, the GDPR made far reaching changes which increased the compliance burden on organisations and strengthened the rights of individuals.

The effects of the GDPR have been felt far beyond the European Union and the European Economic Area. Not only has the GDPR served to "raise the bar" for privacy legislation globally but its extra-territorial reach has meant that organisations outside the EU/EEA cannot afford

to ignore its requirements. This is all the more so when the consequences of non-compliance can result in significant fines, compensation claims by individuals and material damage to an organisation's reputation.

This guide provides an introduction to the GDPR and general information on complimentary national laws which have been adopted by many EU Member States. It goes on to consider significant cases that have come before EU national courts and fines which have been imposed by EU national data protection regulators. Needless to say, the approaches adopted can differ markedly from one

Member State to another and important lessons have been learned along the way.

This guide goes on to highlight data privacy laws that have been adopted in a number of other jurisdictions, including the UK, the US, China and India. Brexit has, of course, added a layer of complexity with the UK having adopted its own, essentially similar, "UK GDPR". Many other jurisdictions have been heavily influenced by the GDPR when implementing new, or updating existing, data privacy laws. In a world where international transfers of data take on ever greater significance, the extent to which other countries' data protection laws provide for comparable safeguards to the GDPR cannot not be overlooked.

We hope this guide is of assistance. Please do not hesitate to contact any of the experts listed if you would like to know more.



David Gourlay
Partner at MacRoberts LLP



david.gourlay@macroberts.com



[David Gourlay | LinkedIn](#)



Joris Lensink
Chairman Interact Law
Partner at De Vos & Partners



jlensink@devos.nl



[Joris Lensink | LinkedIn](#)

David Gourlay

Joris Lensink

02 GDPR

General situation

The General Data Protection Regulation (or the GDPR as it is more commonly known) was adopted in May 2016 and applied directly in all EU and European Economic Area Member States (EEA) from 25th May 2018. This European legislation strengthens Europe's already strict laws around what organisations can do with people's personal data, it gives individuals more information and control over how their data is collected and requires organisations to justify everything that they do with it. Furthermore, it harmonises the previous national data protection schemes within the EEA, giving organisations clear rules on what they can and can't do with personal data.

The impact outside of the EU / EEA

While the GDPR is European Union legislation, it has a huge effect on organisations outside of the EEA, including the UK and the US. The GDPR protects data belonging to EU citizens or residents, therefore it applies to global organisations that handle their data via targeting or monitoring and they must appoint an EU representative if they have no presence in the EU

Controller and Processor

These two definitions are central to the application of obligations to organisations under the GDPR. Obligations will vary depending on whether you are considered a controller, joint controller or processor. Controllers – These are the main decision makers

who determine the purposes and means of the processing of the personal data (i.e. the "why" and the "how" of processing). As a result, they are subject to stricter obligations under the GDPR. The controller can act alone or jointly with others.

Processors - These are organisations that act on behalf of, and only operate on the instructions of, the relevant controller. Processors do not have the same level of obligations as controllers.

For example, Volkswagen will have a website that collects data on the pages their prospective customers visit. This will likely include the link they entered the site through, the pages they visited, and how long they stayed on each page. Volkswagen is the data controller as they decide how all of this information will be used and processed, and for what purposes. Hypothetically, Volkswagen uses Google Analytics to find out which of their pages are most popular and, as a result, which of their products is most appealing. This helps them plan their future advertising strategies. Google Analytics would be the data processor as they have no ownership over the data, nor do they have influence over the purpose of its processing.

There are also particularly sensitive types of personal data, known as special category data, which are given increased protection under the GDPR. ”

What is personal data?

Personal data under the GDPR is any information that relates to an identified or identifiable person who could be identified, directly or indirectly based upon the available information. Examples include; names, dates of birth, ID numbers, email addresses, online identifiers, photographs, religious beliefs and location data.

What is processing?

Processing is a very broad concept and is simply defined as "any operation or set of operations" that is performed on the personal data, whether by automated means or not. This includes but is not limited to; collection, recording, organisation, structuring, storage, adaptation, retrieval, consultation, combination, restriction, erasure and destruction of personal data.

GDPR focus

The GDPR aims to increase public trust by giving European citizens and residents greater control over how their personal data is used. This is achieved by empowering them with a number of rights over their own data such as the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and rights in relation to automated decision making and profiling. It is anticipated that organisations that truly "get" GDPR rights will enhance their reputation and build better trusted relationships with existing and potential consumers.

Consent vs. information

Consent is one of six lawful bases for processing personal data. For processing based on consent to be lawful, consent must be "freely given, specific, informed and unambiguous". This means that the individual concerned should complete a demonstrable affirmative action acknowledging consent, such as clicking an opt-in box when visiting a website. Before doing so they should have been provided with the appropriate information to make this decision i.e. who will be processing their data and for what purpose, this is usually addressed in a privacy policy. Pre-ticked boxes are not acceptable.

People tend to focus on consent as the key basis for processing, but it is arguably the weakest as consent can be withdrawn at any time by the

individual concerned. Organisations can also lawfully process data when they have a contractual or legal obligation, when it is necessary to protect an individual's vital interests, when it is within the public interest or when the data processing is for the legitimate interests of the controller or another party.

There are also particularly sensitive types of personal data, known as special category data, which are given increased protection under the GDPR. These comprise data concerning an individual's health or sexual orientation or activity; that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; that is genetic data or biometric data.



Such special category data must be handled with enhanced care by those who wish to process it. Not only do they need to meet a general legal basis for processing data, they must also meet more stringent requirements such as, for example, the data subject giving their 'explicit consent' or the processing being in the 'vital interests' of the data subject, where they are incapable of giving direct consent.

International transfers of data

The GDPR restricts the transfer of personal data outside of the EEA, unless the country in question is considered to provide adequate levels of protection for personal data. Where a country is considered to offer appropriate safeguards for personal data the European Commission will issue an adequacy

decision, a formal acknowledgement that it is considered safe to transfer data to the country in question. A partial adequacy notice was previously applicable to organisations in the USA who were signed up to a 'privacy shield' scheme, however this was ruled invalid in the Schrems II case (see below). For those organisations outside of the EEA that wish to participate in transfers of personal data from the EU or transfers of EU data, they must incorporate additional safeguards. 'Standard Contractual Clauses' ("SCCs") approved by the European Commission are often entered into by organisations to allow for the international transfer of personal data outside the EEA. This is a rapidly evolving area and organisations should exercise care when engaging in international data transfers, with the ultimate goal of ensuring that any recipient of data in a third country respects in full the Essential Guarantees on privacy, as defined by EU data protection authorities.

GDPR breaches

A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. For example, an accidental update of a database that leads to incorrect data becoming part of an individual's records. If you detect a breach, then you may be required to notify the national regulator within 72 hours and, where the breach may result in a high risk to individuals, to notify the individuals affected without undue delay.

GDPR application to non-EU processors and data controllers

The GDPR extends its territorial reach outside of the EEA in relation to two types of business activities. These are data processing activities relating to: 1. Offering goods or services to individuals situated in the EU; and 2. Monitoring the behaviour of

such persons. As such, data controllers and data processors outside of the EEA whose processing activities relate to such business activities are also subject to the rules set out in the GDPR. This is commonly known as its 'extra-territorial effect'.

Differences in ancillary legislation among EU Member States

The GDPR leaves the possibility for national legislation to specify the rules contained therein, expressly allowing for further specifications or restrictions. This has led to the existence of complementary GDPR legislation in several Member States. You will find details of this legislation below.



Bulgaria

The GDPR was implemented directly in May 2018. In addition, the national Personal Data Protection Act (in force since 2002) was amended in February 2019 to align with the GDPR.

The Personal Data Protection Act does not introduce major differences compared to the provisions of the GDPR, but it adapts certain provisions such as:

- Personal data of children up to 14 years old can be collected and used only with the consent of their parents/ guardians. If the children are of the age of 14 or older no additional consent is required;
 - Personal data can be used by media after careful review of the balance between data protection and freedom of expression and information;
 - Employers must have strict procedures for use of personal data of employees and job applicants and duly inform them for the applicable terms and technical measures for storage and use of personal data.
- In addition the collection and use of different types of personal data is regulated by:
- E-Commerce Act (regarding the use of cookies);
 - Electronic Communication Act (regarding the digital services);
 - Labour Code and its regulations (regarding type of personal data and term of the storage for the purposes of the social security system);
 - Health Act (regarding special personal data for medical status);
 - Law on Credit Institutions and its regulations (regarding bank secrecy);
 - Tourism Act;
 - Insurance Code (regarding use of medical personal data);
 - Criminal Code.

As per art. 79 GDPR in Bulgaria personal data subject rights are both exercisable through the judicial system and enforced by the Commission for Personal Data Protection. In case of fine or obligatory instruction to be implemented the respective entity/ individual can object the act of Commission of Personal Data Protection before the court.



CEE Attorneys
Alexander Sazdov - Partner



alexander.sazdov@ceeattorneys.com



[Alexander Sazdov | LinkedIn](#)

Belgium

Belgium adopted the Law on the Protection of Individuals with regard to the Processing of Personal Data on 5 September 2018 (Act of 30 July 2018 on the Protection of Natural Persons with Regard to the Processing of Personal Data), which implements the GDPR at Belgian level, while providing for some specific provisions:

- Lowering the age of digital consent from 16 to 13 years for the processing of digital data collected during the dematerialised provision of remote services
- Compliance with additional conditions for the processing of genetic, biometric or health data, namely the obligation to draw up a list of the categories of persons having access to such data and their function, to make this list available to the Belgian Data Protection Authority and to ensure

that these persons respect the confidentiality of such data - Difficulty under Belgian law to use genetic, biometric and health-related data processing in the context of employment law. An employer will find it difficult to oblige his/her employees to accept biometric authentication systems. The situation will have to be examined on a case-by-case basis - Compliance with additional obligations regarding the processing of data for historical, statistical or scientific purposes

- Compliance with additional conditions also in the case of the collection of data on criminal convictions and offences
- Extension of the cases in which the appointment of a data protection officer is mandatory
- The use of to the action for an injunction, with reduced deadlines (including under penalty of fines) and damages is generalised, and can be brought by the person affected by the use of personal data as well as by the Data Protection Authority, but also by an organisation or association active in the field of data protection which has been asked to be represented by the person concerned
- Specification of possible sanctions, and in particular, Belgian law considers the violation of data protection legislation to be a criminal offence, the consequence of which is in some cases criminal, fines.

Other sanctions of the GDPR are also included in the Belgian law, such as administrative sanctions (which are however not applicable to public authorities)



Everest Law
Stéphane Bertouille-Senior Partner

 stephane.bertouille@everest-law.eu

 [Stéphane Bertouille | LinkedIn](#)

Croatia

The GDPR was implemented in Croatia by the Act on the Implementation of the General Data Protection Regulation (Official Gazette no. 42/2018, "the GDPR Implementation Act"), which entered into force on 15 May 2018. The GDPR Implementation Act is in line with the main international standards and principles of personal data protection. There are also other Croatian acts which provide more specific rules for the processing of employee data, such as Employment Act (Official Gazette No. 93/2014, 127/2017, 98/2019), which entered into force on 1 January 2020, and the Occupational Safety Act (Official Gazette No. 71/2014, 118/2014, 154/2014, 94/2018, 96/2018), which entered into force on 1 November 2018.

Croatia as well prescribes some legal provisions that specify the requirements of the GDPR, such as:

- processing special categories of personal data, including biometric and genetic data,
- processing for secondary purposes,
- processing for official statistical purposes, and
- processing personal data in the employment context.

With regard to the rules on the processing of special categories of personal data, including biometric and genetic data, the GDPR Implementation Act only contains provisions introducing further restrictions, such as prohibition of the processing of genetic data for the purpose of assessing the possibility of contracting a disease and other health aspects of the data subject in the context of the conclusion of life insurance agreements.

With respect to processing of data for secondary purposes, all secondary processing must be in compliance with the GDPR, but the GDPR Implementation Act allows:

- further processing of personal data for official statistical purposes,
- secondary processing of data collected through video surveillance if it constitutes evidence in court or other equivalent proceedings.


In the context of processing for official statistical purposes, bodies compiling official statistics are not obliged to grant data subjects the right of access to personal data, the right to rectify personal data, and the right to restrict the processing of personal data to ensure that the purpose of official statistics is achieved, but only to the extent that such rights may hinder or seriously jeopardize the achievement of those purposes and where such exemptions are strictly necessary to achieve those purposes.




The GDPR Implementation Act provides specific rules for the processing of personal data in employment context, such as:


- the processing of biometric data on employees, and
- the use of video surveillance in the workplace. The processing of biometric data on employees is allowed for purposes of recording working hours and entering and leaving official premises if required by law or if such processing is carried out as an alternative to another solution, provided that the employee has given his/her explicit consent in accordance with the provisions of the GDPR.

Surveillance of the workplace is only allowed if necessary and justified for the protection of persons and assets, but only if the interests of the data subject do not override the necessity of the data processing by video surveillance.



CEE Attorneys
Tena Tomek - Partner

 tena.tomek@ceeattorneys.com

 [Tena Tomek | LinkedIn](#)

Czech Republic

In April 2019, the Czech Republic approved Act No. 110/2019 Coll., On the Processing of Personal Data (the "Act"), which regulates more detailed provisions on the processing of personal data under the GDPR Regulation. The Act also establishes the position of the Czech Data Protection Authority (Office for Personal Data Protection), which now has clearly defined powers to enforce sanctions for non-compliance with rules set by legislation in the field of personal data protection. The Act includes the following specifications:

- regulates an exception to the obligation to assess the compatibility of purposes when securing protected interests
- stipulates that any child acquires the ability to grant consent to the processing of personal data in connection with the offer of information society services by the age of fifteen (the Act copies the 15-year old limit, which is set for both civil and criminal liability of a child in the Czech Republic)
- contains the exemption from the obligation to assess the impact of the processing of personal data on the protection of personal data if the law imposes an obligation on him to carry out such

processing of personal data

- describes how to comply with information obligations
- defines the concept of public body, which is missing in Article 37 of the GDPR
- contains exceptions to the imposition of sanctions on public institutions and bodies
- reflects the specificity of the processing of personal data for scientific and historical research, or for statistical purposes and the processing of personal data for journalistic purposes or for academic, artistic or literary expression - sets a basic standard with which these categories of controllers should approach the processing of personal data, and requires, inter alia, their storage in an anonymized form, i.e. so that the information cannot be assigned to a specific data subject whenever possible with regard to their activities
- introduces new factual substances of offenses, consisting in breach of obligations stipulated by the Personal Data Processing Act itself, and also provides for sanctions for them
- limits the maximum amount of the fine that may be imposed in connection with the breach of certain obligations within the framework of personal data protection to CZK 10,000,000. The Act adds the chapters not directly linked to the implementation of the GDPR, dedicated in full to:
 - processing of personal data by the competent authorities for the purpose of preventing, searching for or detecting criminal offenses, prosecuting criminal offenses, enforcing penalties and protective measures, ensuring the security of the Czech Republic or ensuring public order and internal security, including searches of persons and objects;
 - processing of personal data in ensuring the defence and security interests of the Czech Republic;
 - further processing of personal data which are to

be or are entered in the register or the processing of which takes place wholly or partly in an automated manner, provided that the personal data are not processed by a natural person in the course of exclusively personal or domestic activities.



CEE Attorneys
Zdeněk Tomíček - Partner



zdenek.tomicek@ceeattorneys.com



[Zdenek T. | LinkedIn](#)



Denmark:

In Denmark, a new Data Protection Act, (Law no. 502) was approved on May 23, 2018. The Data Protection Act supplements the implementation of the GDPR. Among other things, the Data Protection Act governs the enforcement of the GDPR in Denmark. Today, it is not possible for the Danish Data Protection Agency "Datatilsynet" (the independent authority that supervises compliance with the rules on protection of personal data) to issue administrative fines. This will only be possible when the level of sanction for breach of the individual articles of the GDPR is sufficiently clarified in case law.

Additionally, the Data Protection Act contains the following additional provisions:

- Personal data can be included in the data processing of private data controllers if they meet the requirements for exceptions to the ban on the processing of sensitive personal data. The act also specifies that social security numbers may not be published.
- The age limit according to GDPR art. 8 regarding information society services' processing of

children's personal data has been reduced from 16 years to 13 years. If the child is under 13 years of age, the consent or approval of the holder of custody of the child must be given.

- GDPR also applies to information on deceased persons for up to 10 years from the death of the persons concerned, which is a significant difference from GDPR which does not cover information on deceased persons.
- Data protection advisers appointed in accordance with art. 37 is subject to professional secrecy.

It is not possible for the Danish Data Protection Agency "Datatilsynet" to issue administrative fines.

This will only be possible when the level of sanction for breach of the individual articles of the GDPR is sufficiently clarified in case law. ”

Furthermore, an act on television surveillance has been adopted, which clarifies that the regulation also applies to any form of processing of personal data in connection with television surveillance.



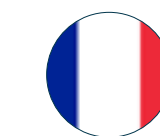
Advodan
Mette Asmussen - Lawyer



meas@advodan.dk



[Mette Asmussen | LinkedIn](#)



France

In France, the law known as "Informatique et Libertés" n°78-17 of 6 January 1978 governs the protection of personal data. In order for French law to be in compliance with the GDPR, the law dated 20 June 2018 (Law no. 2018-493) modified the so called Loi Informatique et Libertés. It appears that the French legislator chose to transpose the GDPR quite strictly in order to move towards homogenisation at European level. For example, some provisions of the law simply refer to those of the GDPR, while others take up the provisions of the GDPR, sometimes with some minor adjustments.

Thus, the Law no. 2018-493 essentially adapted the GDPR on the following rules, among others:

- The scope of application of the national law, which is now applicable to any individual residing in France, including when the data controller is not located in France. However, when one of the processing operations referred to in Article 85(2) of the GDPR is involved (freedom of expression and information), the national law applicable shall be the one to which the data controller is subject when he is established in the E.U. (Article 3 of the Loi Informatique et Libertés).
- The clarification of prior formalities,
- The implementation of processing,
- The processing of criminal data,
- The rights resulting from Articles 15, 16 and 18 to 21 of the GDPR are not applicable for the processing of archival, research and/or statistical purposes (Article 14 of the Loi Informatique et Libertés),
- The threshold for digital minority provided by Article 8 of the GDPR has been set at the age of 15 in France, and
- New procedures for exercising the right of appeal, for the data subject and for the French Commission Nationale de l'Informatique et des Libertés (CNIL)

(the French national authority for the protection of personal data whose powers of control and sanction have been reinforced).

Some provisions of the law simply refer to those of the GDPR, while others take up the provisions of the GDPR, sometimes with some minor adjustments. ”

Finally, Decree no. 2019-536 of 29 May 2019 entered into force on 1 June 2019 and completes the compliance of the Loi Informatique et Libertés with the GDPR. It specifies amongst other things, procedural rules before the Commission Nationale de l'Informatique et des Libertés (CNIL)



Cohen Amir-Aslani Avocats
Ségolène Dugué -General manager

 s.dugue@caa-avocats.com

 [Ségolène Dugué | LinkedIn](#)



Germany

Germany approved on 25 May 2018 the new Federal Data Protection Act (Bundesdatenschutzgesetz - BDSG), which adopted German data protection legislation to GDPR and made further specifications allowed by GDPR. This includes the following regulations:

- BDSG applies, if controller or processor process personal data inside Germany; this is not in line with the principle from Art. 3 para 1 GDPR ruling that GDPR applies no matter whether processing of

personal data takes place in the EU;

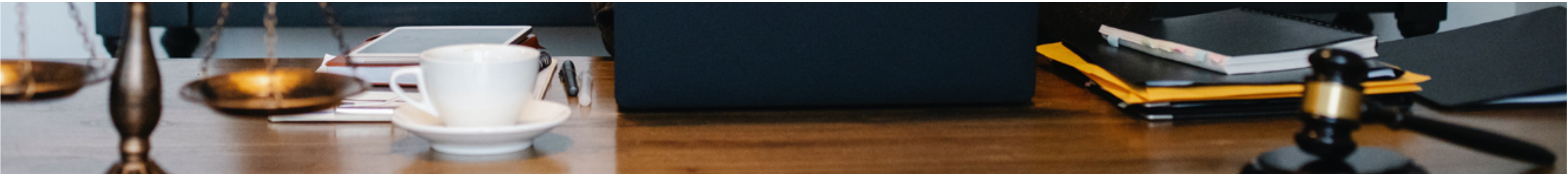
- BDSG provides for national legislation mentioned in Art. 9 para 2 b) and h) GDPR for processing special categories of personal data in connection with rights or obligations from German Social Security legislation or with assessing employees' working capacity;
- BDSG provides for further preconditions for a freely given consent by employees to process their personal data within the framework of the employment contract; freely given consent is deemed to be given only, if employee gains an economic or legal advantage by its consent, which has the consequence, that employee's consent is an unsecure basis for the processing of personal data;
- BDSG provides, beyond the requirement in GDPR, that controllers or processors have to have a Data Protection Officer without further preconditions, if they regularly employ at least 20 people, who process personal data on a steady basis;
- BDSG provides specific legislation for processing personal data in a scientific, historical, statistical or archiving environment;
- BDSG provides for penal sanctions in case of certain severe infringements of GDPR according to the opening clause in Art. 84 GDPR.



ljh Lindlbauer PartmbB
Christian Heimerl

 christian.heimerl@ljh-law.de

 [Christian Heimerl | LinkedIn](#)





Greece

Greece adopted the General Data Protection Regulation (GDPR) into its national legal order through the law No. 4624/2019 on the protection of natural persons with regard to the processing of personal data on 29 August 2019. The following provisions shall be considered as the main points of the Greek Law:

- The processing of underage's personal data, when information society services are offered directly to them, shall be legal only if they have reached the age of fifteen (15) and give their consent, otherwise the consent of their legal representative is required.
- The operation and the duties of the competent supervisory authority, namely the Hellenic Data Protection Authority are determined.
- The Hellenic Data Protection Authority shall not be competent to monitor personal data processing operations carried out by judicial and prosecutorial authorities in the context of their judicial function, as well as operations for the processing of classified personal data carried out for activities relating to national security.
- A distinction between private and public entities as controllers is introduced. Furthermore, for personal data processing by public entities, which do not fall within the scope of the GDPR, the latter applies accordingly.
- The processing of genetic data for health and life insurance purposes is prohibited.
- The further processing of personal data, for example in the case of processing for a purpose

other than the one for which they were originally collected, is permitted only if the subsequent processing is compatible with the purposes of the initial collection, in accordance with the principle of limitation of the purpose in accordance with GDPR.

- The purposes for which the processing of personal data is permitted in the context of employment in the private and public sectors are defined. Especially the employees' personal data may be processed for the purposes of the employment contract at the stage prior to the conclusion of it, during its term, but also after its expiry, if necessary for the purposes of the employment contract.
- Exceptions and deviations from the GDPR with regard to the right to freedom of expression and information, including processing for journalistic purposes and for academic, artistic or literary expression purposes are introduced.
- There is no reference to the adequate safeguards set out in Article 10 of the GDPR on the rights and freedoms of data subjects in the processing of personal data relating to criminal convictions and offences are failing.
- Extensive restrictions on the rights of subjects have been stated.



Politis & Partners
Emmanouil Savoidakis - Senior Associate

 esavoidakis@politispartners.gr

 [Emmanouil G. Savoidakis | LinkedIn](#)

Hungary

The amendment of the Act CXII of 2011 on Informational Self-Determination and Freedom of Information ('Privacy Act') entered into force on July 26, the aim of the modification was to regulate certain areas left open by the GDPR.

The new regulation is based on a new section placed among the general provisions of the Act, which lists in full the provisions of the Act applicable to data processing covered by the GDPR. The provisions listed there complement the rules of the GDPR.

The aim of the modification was to regulate certain areas left open by the GDPR. ”

Under the new provisions, the Act shall apply if the main establishment or the only place of processing activity within the EU of the data controller is in Hungary or, a data processing operation performed by the data controller or the data processor acting on its behalf or at its disposal relates to the provision of goods or services to data subjects resident in Hungary or is related to the observation of the behaviour of the data subject within the territory of Hungary.

This Act also regulates the processing of personal data for the purposes of law enforcement, national security, and defence purposes, where the GDPR is not applicable.

The Act also provides for an extension of the material scope of the GDPR as according to Paragraph (4) of Article 2 of the Act the Article 4 and Chapters II-VI and VIII-IX of the GDPR shall be

compulsory applied in case of paper-based data processing which is not kept in records.

The main rules implemented by the Act are as follows:

- It appoints the Hungarian National Authority for Data Protection and Freedom of Information to perform the tasks and exercise the right of the supervisory authority according to the GDPR in respect of legal entities under the jurisdiction of Hungary.
- It is obligatory to review the need for data processing every three years, if the law or local government decree, on which the data management is based, does not prescribe a compulsory periodic review.
- The Data Protection Officer shall be bound by the obligation of professional secrecy.
- The amendment clarified the rules of judicial enforcement. A person complaining to the supervisory authority regarding a violation of data protection rights by a data controller or processor may, simultaneously, seek judicial redress.
- The burden of proof lies with the controller. If the data owner initiates legal proceedings, the burden of proof does not lie on him, but the controller or processor must prove that the data owner's rights have not been violated.
- The Act provides for the possibility for the owner of the data to appoint in written form a person who is entitled to exercise the data protection rights for five years after the death of the data owner. Some of these rights may be exercised by close relatives even without such appointing document.



CEE Attorneys
Aliz David - Partner



aliz.david@ceeattorneys.com



[Alíz Dávid | LinkedIn](#)

Italy

Italy approved in August 2018 the Legislative Decree 101/2018, which complements the enforcement in Italy of the GDPR by extensively amending Legislative Decree 196/2003 (the so called Privacy Code). In addition to govern the role and powers of the Italian Regulator (Garante per la Protezione dei Dati Personali), it includes the following specifications:

- Establishes that the processing of the personal data of a child in relation to the offer of information society services based on consent shall be lawful where the child is at least 14 years old
- Includes a detailed list of relevant public interests in relation to the processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
- Expressly establishes that the data processed violation of the relevant data protection legislation are 'unusable'
- Addresses the matter of personal data relating to deceased persons



- Declares that consent is not due when processing personal data contained in curricula vitae
- Establishes additional requirements for certain specific types of processing (genetic data, biometric data, health data, data relating to criminal convictions and offences, data concerning a natural person's sex life or sexual orientation, medical prescriptions, public statistics and archiving,

scientific research and statistics)

- Establishes additional security requirements for publicly available electronic communications services providers
 - Includes specification for the limits to the exercise of data subjects' rights, specifically in the field of justice
 - Includes a new series of criminal offences related to the violation of data protection legislation
- The Privacy Code does not provide for any rule of applicability nor it specifies the geographical scope of application of the Italian ancillary legislation.



Tonucci & Partners
Francesco Marchini - Partner



fmarchini@tonucci.com

Luxembourg

The GDPR was implemented in Luxembourg by the law of 26 July 2018 (the "2018 Law"). The 2018 Law repealed the previous Luxembourg national law on the protection of personal data dated 2 August 2002. The 2018 Law has been published in the Luxembourg official gazette on 16 August 2018 and came into force on 20 August 2018.

The 2018 Law does not introduce major differences compared to the provisions of the GDPR, but it applies the options offered by the GDPR to the States members to adapt certain provisions and to define exemptions and derogations. In this respect, the 2018 Law contains specific rules when the GDPR allowed local deviations like on:

- the freedom of information and the freedom of expression; and
- the processing of personal data for scientific or

historical research purposes or statistical purposes. The 2018 Law also specifies the structure, the role, the missions and the power of sanction of the Luxembourg national commission on data protection (the "CNPD"). In addition to referring to the sanctions provided for in article 83 of the GDPR, the 2018 Law also grants specific powers to the CNPD. In fact, the 2018 Law authorises the CNPD to impose a daily penalty payment to a data controller (i) until the CNPD has received the documents that has requested in accordance with article 58 of the GDPR and (ii) in the event that a data controller does not respect a decision given by the CNPD, in order to force such data controller to comply with the CNPD's decision.

In addition, with the implementation of the 2018 Law, the Luxembourg legislator had to decide if the provisions of article L261-1 of the Luxembourg labour code shall remain. This article provided that the monitoring of employees in workplaces was subject to a prior authorisation of the CNPD and also contained strict provisions which had to be complied with. After lengthy debates, the Luxembourg legislator decided to amend article L261-1 by removing the need to obtain the prior authorisation of the CNPD, which demonstrates the will of the Luxembourg legislator to be closely aligned with the GDPR.



VANDENBULKE
Valérie Kopéra - Partner

 vak@vdblaw.com

 [Valérie Kopéra | LinkedIn](#)

The Netherlands

In The Netherlands, the GDPR is complemented by the Dutch GDPR Implementation Act ("Uitvoeringswet Algemene Verordening Gegevensbescherming"). In addition, there are a number of special laws regulating the processing of personal data. The relevant supervisory and enforcement authority is the Dutch Data Protection Authority ("Autoriteit Persoonsgegevens"). In both civil law as well as administrative law cases the Dutch Courts interpret and rule on GDPR legislation.

The supervisory and enforcement authority is the Dutch Data Protection Authority ("Autoriteit Persoonsgegevens").

The Dutch GDPR Implementation Act contains rules on, among others:

- the legal representative's consent;
- processing special categories of data and its lawful bases;
- processing criminal data;
- processing the national identity number;
- automated individual decision making;
- exemptions to the data subject's rights and controller's obligations;
- exemptions for journalistic, academic or archiving purposes;
- the organization and powers of the Dutch Data Protection Authority.

Special laws include legislation regulating, among others:

- the processing of criminal data by criminal law

- enforcement bodies;
- the processing of personal data for elections and public administration;
 - the processing of personal data for social security;
 - the processing of personal data by healthcare providers;
 - telecommunications, direct marketing and cookies.



De Vos & Partners
Jasper Hulsebosch - Partner

 jhulsebosch@devos.nl

 [Jasper Hulsebosch | LinkedIn](#)



Lisanne Bruggeman

 lbruggeman@devos.nl

 [Lisanne Bruggeman | LinkedIn](#)

Romania

The GDPR is directly applicable in Romania since the 25th of May 2018. Law no. 190- entered into force on the 1st of August 2018 (the "Law 190"), establishes the measures necessary for the implementation, at the national level, of the provisions of art. 6 paragraph (2), art. 9 paragraph (4), art. 37-39, 42, 43, art. 83 paragraph (7), of art. 85 and art. 87-89 of the GDPR.

Thus, Law 190 did not introduce major differences compared to the provisions of the GDPR, but contains specific rules when it comes to:

• the use of monitoring systems through electronic communication means and/or video surveillance in the workplace

Thereby, the processing of employees' personal data in such a situation, for the purposes of the legitimate interests pursued by the employer, is permitted only if:

- the employer has made compulsory, complete and explicit prior information to the employees;
- legitimate interests pursued by the employer shall be duly justified and shall prevail the interests or rights and freedoms of data subjects;
- the employer consulted the union or, where appropriate, the representatives of the workers before the introduction of monitoring systems;
- other less intrusive forms and ways to achieve the goal pursued by the employer have not previously proven effective;
- the period of storage of personal data is proportional to the purpose of processing, but not more than 30 days, except for situations expressly regulated by law or duly substantiated cases.

• processing of national identification number (IDN)

The processing of IDN is allowed on the basis of legitimate interest pursued by the controller (art. 6(1) lit. f) of GDPR), provided that the controller takes the following guarantees:

- implements adequate technical and organizational measures (in particular, complying with the data minimization principle), as well as ensures the security and confidentiality of the processing of personal data according to the provisions of art. 32 of the GDPR;
- appoints a data protection officer (DPO), in accordance with the provisions of Law 190;
- establishes retention periods for IDN processing, taking into account the nature and purpose of such processing;
- makes periodic trainings with the persons dealing with IDN processing.

- **processing of genetic data, biometric data or health data**

The processing of genetic, biometric or health data for the purpose of automated decision-making or profiling is permitted with the explicit consent of the data subject or, if the processing is carried out under explicit legal provisions, with appropriate security measures for protection of data subject rights, freedoms and legitimate interests being in place.

The processing of health data carried out for the purpose of ensuring public health (as defined under (EU) Regulation no. 1338 / 2008 on Community statistics on public health and health and safety at work), cannot be subsequently performed for other purposes by third entities.

- **processing of personal data and special categories of personal data (in the context of performing a task that serves a public interest)**

Law 190 allows controllers to process this type of special categories of personal data in the context of serving a public interest according to art. 6(1) let. e) and art. 9 let. g) of GDPR, provided that the controller has implemented guarantees similar in nature to those applicable to IDN processing.

The Law 190 provides certain derogations, for:

- the processing of personal data takes place for the purposes of scientific or historical research, for statistical purposes or for archiving purposes in the public interest. Thus, the provisions of art. 15, 16, 18, and 21 of the GDPR do not apply if personal data are processed for scientific or historical research purposes insofar as the rights referred to in those articles are such as to render impossible or to seriously affect the achievement of the specific goals, and the respective derogations are necessary for the achievement of these purposes; while the provisions of art. 15, 16, 18, 19, 20 and 21 of the General Data Protection Regulation do not apply if personal data are processed for archiving purposes



in the public interest, insofar as the rights referred to therein are of a nature to make it impossible or seriously affect the achievement of specific goals, and these derogations are necessary to achieve these goals. These derogations shall be applicable only subject to the existence of adequate safeguards for the rights and freedoms of the data subjects referred to in art. 89 (1) of the GDPR;

- the processing for journalistic purposes or for the purpose of academic, artistic or literary expression – the processing of this data may be carried out if it concerns personal data which have been made publicly manifested by the data subject or closely related to the person's public status or the public character of the facts in which he or she is involved (by way of derogation from the chapters II, III, IV, V, VI, VII and IX of the GDPR;
- the processing of personal and special data by political parties and organizations of citizens belonging to national minorities, non-governmental organizations – this processing is allowed in order for these entities to achieve their objectives, without the express consent of the data subject, provided that appropriate safeguards (referred to in Law 190) are provided.

As regards the sanctioning regime applicable to private sector, there are no differences from the GDPR fining frame. Opposed to it, the Law 190 sets specific sanctions applicable to public authorities/entities for any data breaches committed by these public bodies, establishing a maximum threshold on the fines that might be applied to them, i.e. up to EUR 42,000.

On a separate note, there are several laws dealing with data privacy/electronic communication, which may be of interest, such as:

- Law no. 102/2005 on the establishment, organization and functioning of the National Authority for the Supervision of Personal Data Processing - the supervisory authority for data privacy in Romania ("NSAPDP");
- Law no. 129/2018 amending Law no. 102/2005 and repealing Law 677/2001 (the former law regulating personal data processing before the GDPR);
- Law no. 506/2004 on processing of personal data and the protection of privacy in the electronic communications sector (transposing EU Directive 2002/58/EC);
- Law no. 365/2002 on electronic commerce

(transposing EU Directive 2000/31/EC);

- LAW no. 363/ 2018 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purpose of preventing, detecting, investigating, prosecuting and combating crime or the execution of punishments, educational and security measures, and on the free movement of these data;
- Labour Code no. 53/2003;
- Secondary legislation: decisions issued by the NSAPDP, e.g. Decision no. 174/2018 regarding the list of activities for which a DPIA is required, Decision no. 161/2018 regarding the investigation procedure, Decision no. 133/2018 for handling complaints, Decision no. 128/2018 for the approval of data breach notification template form.



CEE Attorneys
Krisztina Voicu



krisztina.voicu@ceeattorneys.com



[Krisztina Voicu | LinkedIn](#)



In Slovakia GDPR came into effect on 25.5.2018 and just as any other EU regulation it was directly applicable. Along with GDPR a National Act no. 19/2019 Coll. on Data protection came into effect on 25.5.2018. This National Act on Data protection mostly copies provisions of GDPR with slight differences in wording reflecting specifics of wording on National Laws in Slovakia.

National Act on Data protection in Slovakia was adopted in order to synchronize national laws with GDPR and to adopt specific rules for data protection in cases where GDPR allows member states to have a specific regulation.

Besides National Act on Data protection there are other national laws in Slovakia that include specific regulation with regards to data protection, these include:

- Electronic Communication Act;
- Labour Code;
- Act on the Protection, Promotion and Development of Public Health;
- Healthcare Act.

Some of the specific rules are:

- Employer may publish employees name, surname, academic title, position, phone number and e-mail if it is necessary for employees' work;
- It is possible to process and use customers (potential customers) e-mail address for purposes of sending unsolicited commercial communication if the e-mail was provided by customer to controller in context of sale of goods and services;
- Identification number of citizens may not be published, and its processing is strictly limited to cases when the identification is necessary, and it cannot be replaced by other personal data of data

subject;

- Based on decision of National public Health Office Controllers may process personal data of anyone entering premises of their business as a requirement for allowing entrance to the premises;
- Media may process personal data without consent of data subject if the processing is necessary the purpose of informing the public by mass media unless such processing violates data subjects right for privacy or right for protection of personality or if such processing is explicitly forbidden by law or international treaty.



CEE Attorneys
Michal Martinák - CEO and Partner



michal.martinak@ceeattorneys.com



[Michal Martinak | LinkedIn](#)



Spain approved in December 2018 the Organic Law 3/2018, which complements the enforcement in Spain of the GDPR. In addition to govern the role and powers of the Spanish Regulator (Agencia Española de Protección de Datos), it includes the following specifications:

- Declares expressly legitimate interest as legal ground for the use corporate contact details and individual professionals' data
- Also declares legitimate the transfer of data as result of M&A and other similar entrepreneurial operations
- Describes how to comply with information obligations via several layers
- Includes a detailed list of which sectors of activity whose companies are obliged to appoint a DPO
- Establishes additional requirements for certain

specific types of processing (whistleblowing, Robinson lists, video-surveillance, public statistics and archiving and government fines and penalties)

- Includes specification for the exercise of data subjects' rights, specifically in the field of data-blocking
- Includes a full categorization of GDPR infringements

As a final remark, this national law adds a whole chapter not directly linked with the implementation of the GDPR, dedicated in full to what are known as Safeguards On Digital Rights. This chapter include a variety of protective measures to individuals, including the following specific digital rights:

- Net neutrality
- Universal access to internet
- Digital safety
- Digital education
- Protection of minor aged and their personal data
- Rectification of information published in Internet
- Update of information published by digital media
- Privacy in the use of corporate devices, and employees' privacy in the implementation of video-surveillance and geo-location
- Employees' right to digitally disconnect
- Digital rights in collective negotiation by employees' representatives
- Right to be forgotten in search engines and social media
- Portability at social media, and
- Digital last will



ECIJA
Xavi Muñoz - Partner



xmuno@ecija.com



[Xavi Muñoz | LinkedIn](#)



03

GDPR three years after its introduction

Landmark Cases/Fines and their takeaways

Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems Case C-311/18 ("Schrems II") (July 2020) – This case invalidated the EU-US Privacy Shield framework as an international agreement which enabled organisations to transfer personal data to the US. It also cast doubt on the legitimacy of the SCCs as a method of transfer. Organisations seeking to rely on SCCs as a method to transfer personal data internationally will need to verify the level of privacy protection in the recipient country before using them.

Commission on Informatics and Liberty (CNIL- French regulator) fine of Google LLC (Google's French arm) (Jan 2019) – This is the biggest GDPR fine to date (€50 million) issued for various failings under the GDPR. The main one being due to a lack of transparency as individuals were not provided with the appropriate fair processing information necessary to establish why Google was processing their data and for how long it would be kept. Google also failed to meet the standard required for lawful consent when providing personalised advert content. The key takeaways here are to ensure it is easy for users to understand what you intend to do with their data, this should be clearly signposted. Also, for consent to be valid, it must involve affirmative action.

Italian Data Protection Agency Garante's €27.5 million fine of Italian telecommunications operator TIM (January 2020) – This involved an extensive list of violations of the GDPR such as: improper management of consent lists, excessive data retention, improper handling of data breaches, lack of proper consents and violation of individual's rights under the GDPR. The actions of TIM highlight what behaviours organisations should avoid when seeking to comply with the GDPR.

Bulgaria:

There are two landmark cases before the Bulgarian Commission for Personal Data Protection up to today

Commission for Personal Data Protection vs. National Revenue Agency: The Bulgarian National Revenue Authority had a major problem with its data bases and in 2019 personal details belonging to more than five million people was accessed without and distributed on the internet. This is the biggest personal data breach in Bulgaria up to present date. The personal data included names, addresses and contact information, data from individuals' annual tax returns, information relating to their personal income tax position, etc. In



addition the NRA was obliged to improve its cyber security internal rules.

Fine appr. BGN 5 million (€2.61m)

Commission for Personal Data Protection vs. DSK Bank EAD: Bulgarian bank had not implemented proper security measures. So a third party obtained unauthorised access to personal data belonging to more than 33,000 customers of the bank.

Fine appr. BGN 1 million (€511,000)

Croatia:

In Croatia, there have been only two publicly known cases of violations of the GDPR in which a fine was imposed. One of the cases concerns a breach of the GDPR by a bank. Croatian Personal Data Protection Agency (AZOP) fined the bank for violating Article 15 (3) of the GDPR, more specifically for refusing to hand over personal data to the bank's customers. The customers requested a copy of the loan documentation (e.g. repayment schedule, annex to the loan agreement, verification

of interest rate changes) containing their personal data and the bank continuously refused to provide requested document. The bank argued that despite being a data controller, the obligation to provide customers with access to data does not apply because the data is not considered personal data, but rather data in loan documentation to which the Consumer Credit Act applies. The AZOP found that the documentation contained personal data, and the bank was ordered to provide documentation to all customers who requested it. The bank received approximately 2,500 requests from customers who were denied the right to submit copies of personal data. In determining the amount of the fine, the AZOP considered the criteria expressly prescribed in Article 83 (1) of the GDPR; first, the bank's described conduct was deemed to have resulted in a serious breach of customers' rights, which is governed by Article 83 (5) (b) of the GDPR, for which a fine of up to EUR 20,000,000 is prescribed. AZOP also took into account that the breach affected over 2,500 citizens of the Republic of Croatia.

In the other case, the AZOP issued a decision imposing a fine on the security company as a processor for violating Article 32(1)(b), (d) and (2) and (4) of the GDPR. Namely, the controller contacted the AZOP pursuant to Article 33(1) of the GDPR with a

report of personal data breaches that took place in their office. An employee of the processor shared a surveillance screen with a third unauthorized party, after which the footage reached social networks and the media. In deciding on the imposition of a fine as well as its amount, AZOP considered the criteria prescribed in Article 83(2) of the GDPR.

Czech Republic:

Ministry of the Interior / Office for Personal Protection (UOOU-09383/18-17)

For the first time, the Office for Personal Data Protection (the "Office") applied a new provision of the Act (Section 62 (5) of Act), according to which an administrative penalty cannot be imposed on a public authority and a public entity, even though the law has been violated. It was an offense committed by the Ministry of the Interior in connection with the processing of personal data in the population register, the Ministry of the Interior allowed a total of 7,064 unauthorized access to the population register in connection with the authorization agenda under the Act on Verification and Recognition of Further Education Results.

An administrative penalty cannot be imposed on a public authority and a public entity. ”

Furthermore, it allowed a total of 88,491 accesses to data in the population register to a greater extent than stipulated by the Act on Basic Registers and within the system settings of the population register allowed executors access to personal data of all so-called tied persons. Thus, the Ministry of the Interior, as the controller of personal data, did not adopt sufficient measures to prevent unauthorized or accidental access to personal data in the population register. In view of these

serious findings, the Office initiated infringement proceedings against the Ministry of the Interior. Subsequently, the Ministry of the Interior was found guilty of committing an offense. For failing to take or implement measures to ensure the security of personal data processing, thereby violating the legal obligation, a fine of CZK 1.1 million would normally be imposed. On the basis of the filed appeal, the appellate body agreed with the conclusion that the Ministry of the Interior, as the administrator, is responsible for the unauthorized provision of personal data. However, due to the fact that in the meantime the Act entered into force on 24 April 2019, the Office was forced to refrain from imposing such a fine.

Also, the Office imposed the fine on the personal data administrator, who processed the biometric signature of clients in order to simplify the process of concluding and storing contractual documentation. The Office assessed such a procedure as a violation of the principle of processing personal data only to a reasonable, relevant and limited extent in relation to the given purpose (the so-called principle of data minimization) and imposed a fine of CZK 250,000.

Denmark:

In Denmark, we had to wait until the end of March 2019 before the first company was set at a fine, and only on 12 February 2021 was the first judgment handed down by the court in Aarhus.

The first recommendation of fine from the Danish Data Protection Agency were against the taxi company 4x35 with an amount of DKK 1.2 million (approximately EUR 160.000). The company deleted the customer's name after a two-year storage period - but not the customer's phone number. Information about the customer's taxi journey (including collection and delivery addresses) could therefore still be attributed to a specific person via

the telephone number, which was only deleted after five years.

The first court case was against the furniture company ILVA / IDesign. The Danish Data Protection Agency chose in June 2019 to report the company to the police and recommend a fine of DKK 1.5 million (approximately 200.000 Euro). The case related to the company's storage of customers' personal data in an older ERP system. The system processed information about the customers' name, address, telephone number, e-mail and purchase history. There was no registration of use of the information or security breaches. The case concerned only the issue of storage restrictions and the possible sanction for breach of the GDPR.

The court found it proved that there had been a violation of the GDPR since the valid purpose of storage no longer existed. According to the court's assessment, the personal data should have been deleted in accordance with the 5-year rule in the Danish Accounting Act. In relation to the question of sanctions, the following mitigating circumstances were included in the assessment of the sanction:

- The company had no precedent for breach of GDPR.
- Information was in an older and partly phased-out system that was only accessed occasionally.
- No data subject was injured.
- The breach was of a formal nature.
- The company had made quite significant efforts to ensure compliance with the rules.
- The company had only shown negligence and not intent.

The calculation of the fine was based on the specific company's own annual revenue and not the group revenue and was set at DKK 100.000 (approximately EUR 13,500). The judgement has been appealed to the High Court.

France

On December 7, 2020, the French data protection agency (Commission nationale de l'informatique et des libertés or CNIL) fined Google the amount of 100 million euros (60 million euros for Google LLC and 40 million euros for Google Ireland Limited respectively) for three (3) violations of article 82 of the French Law on data processing and Liberties, i.e. (i) depositing cookies without the user's prior consent, (ii) a failure to inform users of the google.fr search engine and (iii) the partial failure of the "opposition" mechanism.

On the same date, the French data protection agency fined Amazon the amount of 35 million euros for two (2) violations of the hereabove mentioned article, i.e. (i) depositing cookies without the user's prior consent and (ii) a failure to inform users of the amazon.fr website.

The French data protection agency justified these amounts because in particular google.fr and amazon.fr websites are used by millions of people. Furthermore, the sanctioned companies had a 3-month delay in order to be in compliance with article 82 of the French Loi Informatique et Libertés, otherwise, the French data protection agency may fine the amount of 100,000 euros per day of default. Moreover, in November 2020, Carrefour France (retail) and Carrefour Banque (bank) were fined 2.250.000 euros and 800.000 euros respectively. Indeed, both companies had been the subject of several complaints to the CNIL. On this occasion, the CNIL found shortcomings in the processing of customers and potential users data relating to:

- Art. 13 of the GDPR: the right to be informed;
- Art. 82 of the French Loi Informatique et Libertés: deposit and use of cookies;
- Art. 5.1.e of the GDPR: obligation to limit the duration of data retention;
- Art. 12 of the GDPR: transparent information,

communication and modalities for the exercise of the rights of the data subject;

- Art. 15, 17, 21 of the GDPR and L34-5 of the French Code des postes et des communications électroniques: right of access, right to erasure ("right to be forgotten"), right to object; and
- Art. 5 of the GDPR: right to a lawful and fair processing of personal data.

Germany

Deutsche Wohnen / Berlin Data Protection Authority

Deutsche Wohnen is one of the largest apartment lessors in Germany. Berlin Data Protection Authority argued, that Deutsche Wohnen had not or not correctly erased personal data of lenders, like employment contracts, tax documents or salary statements. Deutsche Wohnen was demanded several times to erase or not store the personal data longer than permitted, but did not react. Berlin Data Protection Authority issued an Order over a fine in the amount of € 14,5 million.

1&1 / Federal Data Protection Officer

A customer of 1&1, a German telecommunication service provider, was stalked by his former girlfriend via his new phone number at 1&1. She had asked for the new phone number at 1&1 call center by pretending to be the customer's wife. She only had to indicate name and date of birth of the customer to get disclosed the new phone number. Federal Data Protection Officer issued an Order about a fine in the amount of € 9,55 million. 1&1 objected and brought the case to court. Court of first instance in Bonn confirmed infringement of GDPR rules, but reduced the fine substantially to € 900.000.

Delivery Hero / Berlin Data Protection Authority

Delivery Hero, a food delivery service, did not erase personal data of customers in due time and sent infringing advertising emails.

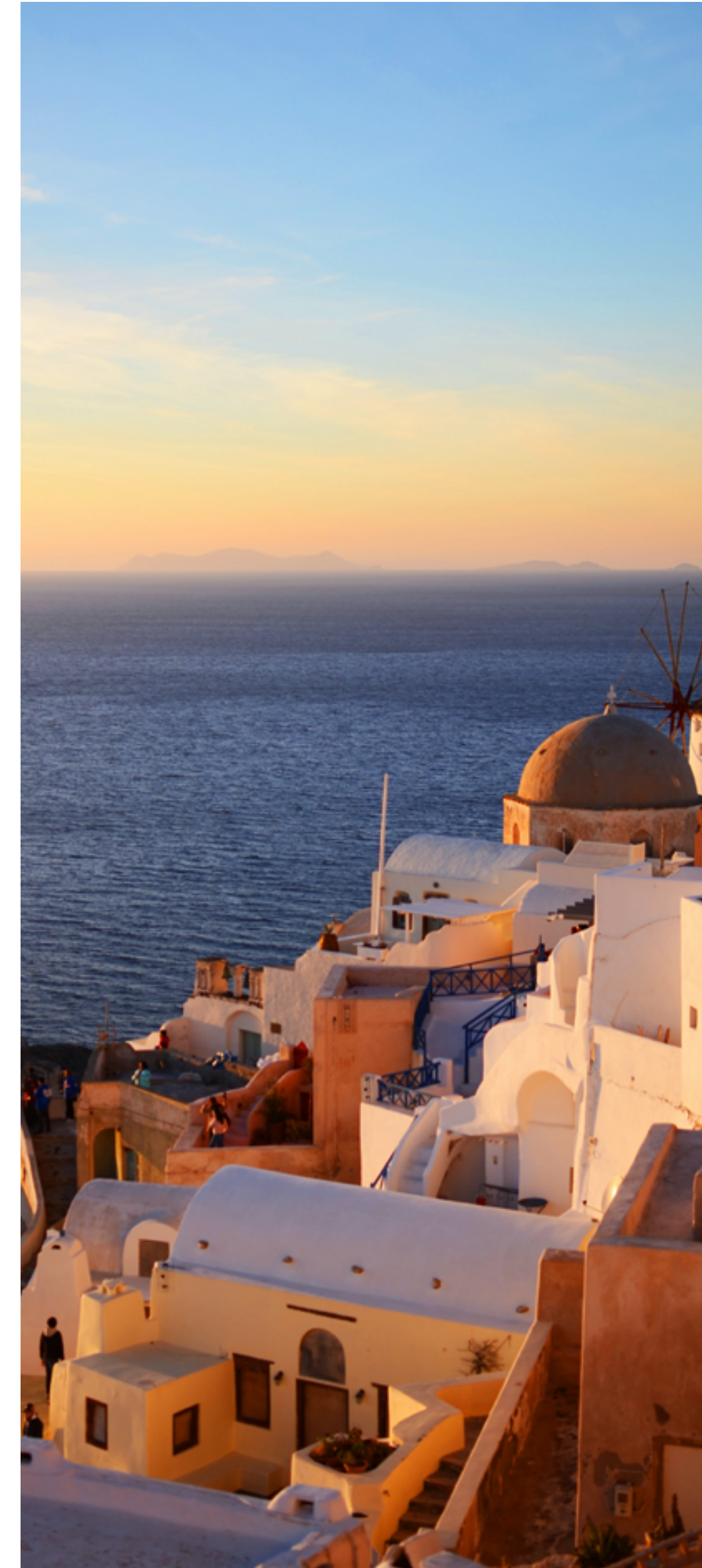
Berlin Data Protection Authority issued an Order about a fine in the amount of € 195.407 for this

Greece

Hellenic Data Protection Authority - Hellenic Telecommunications Organisation S.A. (hereinafter as "HTO") (2019). Two fines of a total amount of EUR 400.000 were imposed to the HTO both for failure to satisfy the right to object and violation of the principle of data protection and for violating the principle of accuracy and data protection already by design in the retention of the personal data of its subscribers. The Authority highlighted that for any matter relating to the provision of electronic communications services which is not specifically regulated in the relevant Law (Law 3471/2006) the GDPR applies.

Hungary:

The record penalty in Hungary so far is HUF 100 million (approx. EUR 280,000). According to the Hungarian National Authority for Data Protection and Freedom of Information the data controller - Digi Távközlési és Szolgáltató Kft. - became aware and immediately reported a data protection incident in connection with the fact that a hacker exploiting the vulnerability of their website www.digi.hu, had access to a large number of personal data of the customers of the data controller, including the names of the data subjects, mother's name, place and time of birth, home address, ID number (sometimes personal number), e-mail address, landline, and mobile phone numbers. Moreover, it has been found that the user data of the administrators were also accessed, therefore an even wider abuse could have happened. Interestingly, the attack was carried out by an ethical hacker who explored the vulnerabilities of various web interfaces not with the intent of abuse but trying to help, he immediately reported the bug



to data controller, along with its technical nature, so the company was able to solve the problem without delay. The authority justified the exceptionally large fine of HUF 100 million emphasizing that the incident occurred due to an error (bug) of which the company had been (may have been) aware for nine years, but did not take any action, disregarding even its own internal regulations.

UPC was able to claim the second largest penalty in 2020. The Authority imposed a data protection fine of HUF 60,000,000 (approx. EUR 170,000) for voice recordings made during personal customer service processes in 24 stores in Hungary. Customers entering the store were informed of the fact that voice recordings are made through the take-a-number system and the warnings were also included in the General Information on their website. In the Authority's view, the legal basis for data processing was missing as the legitimate interests of the customers were not examined, guarantees regarding the rights of data subjects were also not considered adequately; the stated purposes for data protection were not clear, therefore the data process did not comply with the purpose limitation principle; furthermore the data controller failed to provide proper information to the customers and by recording the entire customer service process, the principle of data minimization was also violated.

The Netherlands:

VoetbalTV / Dutch Data Protection Authority (District Court Midden-Nederland, 23 November 2020, ECLI:NL:RBMNE:2020:5111):

VoetbalTV is an internet platform which broadcasts amateur football matches, and processes personal data on a legitimate interest-basis (article 6(1) (f) GDPR). The Dutch Data Protection Authority considers VoetbalTV's interest a purely commercial interest which can never be qualified as a legitimate interest. However, the The District Court

ruled in favor of VoetbalTV that the prior exclusion of a particular interest as a legitimate interest is contrary to European case law. Whether an interest is justified must be assessed under a negative test, which means that the processor may not pursue an interest that is contrary to the law. According to the latest information, the Dutch Data Protection Authority has appealed to this decision.

Plaintiffs / The Dutch State regarding SyRI (The Hague District Court, 5 February 2020, ECLI:NL:RBDHA:2020:865):

SyRI is a legal instrument used by the Dutch government to combat fraud in areas such as benefits, allowances and taxes. Within the SyRI system, (personal) data is linked and analyzed in order to generate risk reports (profiling). The Court ruled that the SyRI legislation violates higher law. More specifically the Court finds that said legislation does not comply with article 8 of the European Convention on Human Rights (ECHR), which protects the right to respect for private and family life, home and correspondence. According to the Court, the SyRI legislation is insufficiently transparent and does not provide for adequate safeguards. In addition, insufficient regard has been paid to the principles of purpose limitation and data minimization. The Court did not assess whether the SyRI legislation conflicts with one or more specific GDPR provisions. The Dutch State did not file an appeal against this decision.

Fines:

Until beginning of 2021, the Dutch Data Protection Authority issued several fines up to € 830.000,=. This includes fines regarding:

- the inadequate securing of medical files by the Dutch hospitals 'OLVG' and 'HagaZiekenhuis') (€ 440.000 resp. € 460.000);
- the unlawful selling of member's data by the Dutch Tennis Association (KNLTB) (€ 525.000);
- the unlawful processing of employee fingerprints

for attendance and time recording purposes (€ 725.000);

- the charging for exercising a data subject's access right by the office for credit registration (BKR) (€ 830.000);
- the late reporting of a data breach by Booking.com. (€ 475.000)

Romania

The Romanian DPA ("NSAPDP") fined three major banks with EUR 130,000, 80,000 and 150,000 due to not implementing appropriate technical and organisational measures. In the first case, the fine of EUR 130,000 was applied to Unicredit Bank S.A. (June 2019) for the controller's failure to implement appropriate technical and organisational measures (and the integration of necessary safeguards) resulting in the online disclosure of IDs and addresses of 337,042 data subjects (and breaching also the principle of privacy by design & privacy by default). Also, Raiffeisen Bank Romania did not observe the necessary security measures required by the GDPR when it assessed the scores of individuals on WhatsApp platform so it was sanctioned with a EUR 150,000 fine.

NSAPDP also issued several other fines for various types of GDPR breaches, such as:

- EUR 170,000 fine applied to Raiffeisen Bank SA and Vreau Credit S.R.L. for violations of art. 32 of the GDPR (insufficient technical and organisational measures to ensure information security); two employees of Raiffeisen Bank S.A. received from employees of Vreau Credit S.R.L., through the WhatsApp mobile application, copies of IDs of natural persons (potential clients of Vreau Credit S.R.L.);
- EUR 2,000 fine (November 2019) applied to Telekom Romania Mobile Communications SA for processing inaccurate date (breaching principles

under art. 5 of GDPR);

- EUR 10,000 fine (December 2019) issued to Hora Credit IFN S.A (a non-banking financial institution) for breaching GDPR principles by disclosing personal data to a wrong recipient;
- EUR 500 fine on a natural person (holding the position of General Secretary within a sector branch of a political party) disclosing on a social network a list of 10 positions of the signatories' and supporters' data (name, surname, signature, citizenship, date of birth, address, series and number of identity card, political option) during the General Council and Bucharest Mayor elections - violating the provisions of art. 32 GDPR on safety of processing and not responding to ANSPDCP requests;
- EUR 2,500 fine applied to an online store for transmission of several unsolicited newsletters;
- EUR 2,500 fine applied to UTTIS INDUSTRIES for not adequately informing the data subjects on using its CCTV system, and for unlawful disclosure of IDN to a third party;
- EUR 15,000 applied for breach of art. 32(1) of the GDPR by World Trade Center Bucharest S.A. relating to security for the processing of personal data; the breach consisted of the failure to take steps to ensure that data is not disclosed to unauthorised persons.

In a summary, during year 2020, NSAPDP received a total number of 5,480 complaints, notifications regarding security incidents, based on which 694 investigations were opened. As a result of the investigations, 29 fines, with a total amount of approx. EUR 185,000, were issued. By comparison, during its investigations in 2019, NSAPDP issued fines in a higher amount, with an aggregate of EUR 474,945.





Slovakia:

In Slovakia data protection rules are enforced primarily by Office for personal data protection and courts. However, there were not too many cases to date and imposed fines are mostly low.

Most prominent were cases where Office for personal data protection fined data controllers for breaches of data processing rules:

Office for personal data protection c/a Slovak Telekom

Slovak Telekom was fined with EUR 40,000 - for insufficient technical and organisational measures to ensure information security. Due to lack of control measures Slovak Telekom distributed contracts of 23 customers to wrong addresses which resulted in breach of their right for data protection. Based on this decision it is clear that controller must adopt appropriate measures to ensure, that contracts containing personal data shall not be made available to third parties.

Office for personal data protection c/a Social Insurance agency

Social Insurance agency was fined 50.000,- EUR for Insufficient technical and organisational measures to ensure information security. Slovak Social insurance agency sent sensitive documents necessary for invalidity pension of their client to Denmark's Social insurance agency through second class mail and the documents were lost during transit. Based on this case controller must chose appropriate means for sending documents that include sensitive personal data.

Office for personal data protection c/a Transport Company of Bratislava

Transport Company of Bratislava was fined EUR 20,000 - for insufficient technical and organisational measures to ensure information security. Transport Company of Bratislava used

cameras in public transportation that recorded unnecessarily wide angles, retention period of 23 days was deemed too long, "monitored space" notice was not linked properly to more detailed information. Conclusions of Office for personal data protection indicate what the office sees as an appropriate extent of data processing for purposes of ensuring public order and crime prevention.



Spain

Spanish Data Protection Agency - AEPD fines two major banks with 5M and 6M Euros for breaches of obligation of information and incorrect use of legitimate grounds of processing (November 2020 and January 2021) - BBVA was object of the first fine due to breaches in obligation to provide information to data subjects in a proper way, since the AEPD considered this bank was providing unclear information about purposes of processing, categories of data processed for each specific purpose of processing, lack of clarity in the explanation of processings based on legitimate interest and profiling. On the other hand, CAIXABANK was imposed the second fine due to inconsistencies in the information provided through different channels used to obtain clients' data, incorrect transfer of data within group companies, incorrect consent mechanism applied to several different processings and incorrect use of legitimate interest as legal ground of processing.



04

Data privacy legislation introduced in other jurisdictions

United Kingdom

England

How has your country/region enacted specific data privacy legislation?

From 1st January 2021, the 'UK GDPR' replaced the GDPR as England and Wales' data protection law through the Data Protection Act 2018 and the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019. Very little was changed between the GDPR and the UK GDPR, meaning that the two remain substantially similar.

How does this compare to GDPR?

The two currently remain substantially the same, with very little difference. The one major difference to date stems from the European Commission's decision to implement updated Standard Contractual Clauses (SCCs). The UK has not yet adopted updated SCCs, so this seems to be the first area of divergence between the two regimes. Indeed, if the UK does not adopt the new EU SCCs then organisations which transfer data from both

the EU and the UK to third countries to which no adequacy decision applies, will need to have two different sets of SCCs in place.

Additionally, on 10 September 2021, the government launched a consultation on reforms to the UK's data protection regime. This consultation presents proposals for bold reform intended to build on the key elements of the UK GDPR, moving towards an "even better data protection regime" that will: support and keep pace with innovation and growth; not compromise on data protection standards whilst removing "unnecessary barriers to responsible data use"; increase certainty regarding the use of data; and improve the Information Commissioner's Office's regulatory remit, including tougher penalties for nuisance calls and text messages.

The UK has not yet adopted updated SCCs



What was GDPR impact on such legislation?

As the UK was subject to the GDPR until 31 December 2020, this question does not really apply.

Significant examples in your country/region: cases, penalties or breaches (if not already mentioned in part 2)

Again, these remain substantially aligned to the EU at the moment, as not much time has passed since the change to the UK GDPR. There have been no recent significant penalties cases. There was a chance the British Airways personal data breach might have been significant, but the fine was reduced due to the effect of Covid-19 on the airline, so was not particularly reportable as a result. There was one other landmark case in December 2020 called Soriano v Forensic News LLC & Ors [2021] EWHC 56 (QB). In this case, Mr Soriano (a British citizen) attempted to pursue six defendants in the USA for breaches of the GDPR. This therefore, tested the territorial reach of the GDPR and its so-called 'international' application to some extent. The court

held that Mr Soriano had no arguable case under the GDPR and that the English Courts were not the 'forum conveniens' for the case.

What are local and international clients' biggest concerns when you are advising about data privacy? What are the main challenges your clients have faced, and which ones will have to face in the future to comply with data privacy legislation?

These will certainly match the concerns facing clients across Europe, as the two regimes have only recently diverged. One issue we have seen arise several times is where a processor in the UK needs to return personal data to a controller in the USA. By reason of the personal data entering the UK, the data becomes subject to the UK GDPR. However, since the Schrems II judgment and the abolition of the Privacy Shield scheme, there is no longer an appropriate forum through which processors can implement safeguards for the return of this personal

data, given that no SCCs exist which govern this scenario.

Very little was changed between the GDPR and the UK GDPR, meaning that the two remain substantially similar. ”

Going forward, immediate concerns centre around whether divergences between the UK and EU privacy regimes will cause the EU to revoke its recently declared adequacy decision, which would be catastrophic for trade between Europe and the UK.



BDB Pitmans
Olivia Mulvany - Associate

 oliviamulvany@bdbpitmans.com

 [Olivia Mulvany | LinkedIn](#)

Scotland

Most prominent breaches

Marriott international (July 2019) – Marriott exposed itself to a major GDPR breach via cyber-attack which was an unintended consequence of their acquisition of the Starwood hotels group in 2016. This data breach, which had affected the Starwood systems since 2014 was not discovered by Marriott until 2018. It involved the exposure of over 339

million guest's records, of which 31 million were residents of the EEA. The renowned hotel chain was eventually fined £18.4 million in 2020, after significant representations were made to the UK regulator (ICO) and mitigating circumstances were taken into account.

British Airways plc (July 2018) – In this instance the well-known British airline was subject to a sophisticated cyber-attack which diverted users' traffic to a "hacker" website which resulted in more than 400,000 customers' personal data being compromised. Upon notifying the UK Information Commissioner's Office they were advised that they could be subject to fines of up to £183 million. However much like in the Marriott case after careful consideration and re-assessment of the ICO's calculation of the fine in line with turnover based bands, a fine of £20 million was imposed.

Impact on extra-EU jurisdictions

Many of the companies involved in these cases and breaches were North American headquartered companies and yet despite being outside the jurisdictional reach of GDPR, they were caught by the reach of the legislation. For example, supervisory authorities imposing punitive fines will give consideration to all legal entities engaged in the economic activity that has caused or relates to a breach, including parent and subsidiary companies, when calculating fines. This was demonstrated in the French case in which the supervisory authority, CNIL, considered the group turnover of Google LLC, including its 70 offices in 50 countries rather than the turnover of its French subsidiary Google France SARL, when imposing the €50 million fine.

Changes in post-Brexit UK

The UK is committed to upholding the standards of the GDPR despite leaving the European Union and has incorporated the Regulation into UK law. This is known as the UK GDPR. This is essentially a

copy of the entire structure of the EU legislation with certain changes and applies to organisation that processes the personal data of individuals inside the UK. Both the UK Government and the EU have recognised each other as adequate allowing transfers of personal data to/from the UK and the EEA without the need for standard contractual clauses.

The new complex framework of international transfers of data: impact on services by cloud computing providers

Third country cloud and IT service providers processing personal data of EU citizens via international data transfers must ensure that the transfers are predicated upon either an appropriate adequacy decision by the EU or that the appropriate safeguards such as standard contractual clauses or binding corporate rules have been put in place by the data controller.



MacRoberts
David Gourlay

 david.gourlay@macroberts.com

 [David Gourlay | LinkedIn](#)



Switzerland

How has your country/region enacted specific data privacy legislation?

The Swiss Federal Act on Data Protection (FADP) and its corresponding ordinance date back to 1992 with the last amendment having come into effect on March 1, 2019. In September 2020 the Swiss Parliament signed off the revised FADP which will to a large extent introduce an alignment of Swiss data protection law with GDPR. The revised FADP is likely to come into force in mid-2022 (date not officially confirmed yet). The FADP applies to federal authorities and private companies. Cantonal authorities and institutions are subject to the cantonal data protection laws at their domicile/seat.

The FADP applies to federal authorities and private companies ””

How does this compare to GDPR?

Whereas most processing principles and obligations are already similar to GDPR, there are two fundamental differences. The first being that under the current and also the revised FADP the processing of personal data is permitted as long as the principles set out in the law are adhered to and the obligations set forth are met. The second difference is the fact that the current FADP not only protects data of individuals, i.e. natural persons, but also data of legal persons. The revised FADP will limit the protection to data of individuals. The current FADP contains the principles of fair and transparent processing adhering to the purposes indicated at the time of collection of the data. Where consent is required, consent must be given freely and based on sufficient information on the purposes of processing. Implicit consent, however,

is permissible under Swiss law as opposed to GDPR. The Swiss Data Protection and Information Officer FDPIC has no sanctioning power, i.e. individuals must bring forth their claims in court or may initiate criminal proceedings in certain cases (wilful intent required).

What was GDPR impact on such legislation?

The revised FADP was very much influenced by GDPR as it will introduce concepts such as privacy by design and default, a data breach notification requirement, accountability requirements such as maintaining a list of processing activities, an active duty to inform data subjects about any processing and its purposes as well as a data portability right. Also, the revised act will introduce a new sanctioning system for data protection law violations. In contrast to GDPR, certain violations are subject to criminal proceedings and a fine of up to CHF 250'000 with the person responsible within a company for the violation in question being held personally responsible. The competent authorities are the cantonal police forces.

Significant examples in your country/region: cases, penalties or breaches

Because the current law has no penalty system and there is no obligation to report breaches there are no significant examples to be reported yet. This certainly will change with the revised law. The most current investigation of the FDPIC concerns a digital vaccination platform which had about 300'000 registered users and which was reported by a team of investigative journalists to lack sufficient technical security measures with health data of the users being easily accessible by third parties. The FDPIC took action end of March 2021 and is currently assessing any potential data protection violations. Under the current law, the FDPIC can, however, only issue recommendations and no sanctions. Hence, if the company refuses to

acknowledge the FDPIC's findings and follow any recommendations issued by the FDPIC, the latter would have to seek a court ruling with the federal administrative court.

The current law has no penalty system and there is no obligation to report breaches [...] This certainly will change with the revised law. ””

What are local and international clients' biggest concerns when you are advising about data privacy? What are the main challenges your clients have faced, and which ones will have to face in the future to comply with data privacy legislation?

Because of the rather weak sanctioning system under the current Data Protection law, compliance with data protection regulation was not a top priority for many companies for a long time. GDPR has changed that mind set and in particular local clients are now keen to be on top of all the new requirements the revised Swiss law will bring. The biggest challenge is likely to bring a structured approach to the documentation and accountability requirements such as list of processing activities, internal data protection guidelines, incident response plan for data breach notifications and reviews of the contracts with processors and sub processors. International clients and local clients that are subject to GDPR, certainly are less concerned because for them there will be only minor adjustments required and they can draw from their expertise gained when preparing for and implementing the compliance measures required by GDPR.



Wenger & Vieli Rechtsanwälte
Claudia Keller - Counsel



c.keller@wengervieli.ch



[Claudia Keller | LinkedIn](#)



Wolfgang Zürcher
Partner



w.zuercher@wengervieli.ch



[Wolfgang Zürcher | LinkedIn](#)



DATA PROTECTION VIS A VIS PRIVACY OF CITIZENS AND IMPACT OF GDPR ON INDIA

India is a country with a population of almost 1.3 Billion in the year 2021 and all set to increase as per the several surveys conducted by the Government agencies till the year 2050. With such vast population comes the details and data of its citizens which is much sought after in the current era of digitisation.

The case of America and how the data can impact even the strongest of the countries and their economies is a classic example at hand. Nobody can forget the Facebook Cambridge data scandal. The data were collected through an app called "This Is Your Digital Life" in the year 2013. Cambridge Analytica used the data to provide analytical assistance to the 2016 presidential campaign in USA and subsequently the Facebook was even fined an hefty amount for exposing the data of its users. In the Indian context, so far as the history of Data Protection is concerned, the Hon'ble Supreme Court of India has recognised the Right to Privacy as a Fundamental Right of its Citizens through its landmark judgment passed by a 9- Judges Bench on 24.08.2017 in JUSTICE K.S. PUTTASWAMY (RETD) VS UNION OF INDIA (2017) 10 SCC 641.

The Hon'ble Supreme Court also made it clear through its decision that the right to privacy is not an absolute right and the right may be restricted only by state action that passes each of the three tests. First, such state action must have a legislative mandate; Second, it must be pursuing a legitimate state purpose; and Third, it must be proportionate i.e., such state action – both in its nature and extent, must be necessary in a democratic society. The Enactment that deals with

protection of data is the IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011 (the "IT Rules"). Under the IT Act and the IT Rules, what is primarily sought to be protected is 'personal information' and 'sensitive personal data or information', i.e. the information related to (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; and (vi) biometric information. However, the information which is freely available in public domain is not considered within the ambit of 'sensitive personal data or information'.

On 25.05.2018, the European Union in order to meet the security concerns that come with digitisation era and to safeguard the individuals control over their personal data and to simplify the regulatory environment for conducting the international business by unifying the regulation within the EU supersedes the Data Protection regulations that were in place since 1995 with the General Data Protection Regulations (GDPR), 2016. Currently in India, we can find some of the below provisions under the IT Act that correspond to the GDPR of EU.

Rule 4 of IT Rules, 2011 deals with the Common data protection security practices and include adoption of internal policies, security audit, adherence to voluntary code of conduct and certification mechanism.

Rule 7 of IT Rules, 2011 deals with the Transfer of sensitive personal data or information by a body corporate in India to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules.

Section 43A of the IT Act, 2000 provides for the grant of compensation which is payable by the body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates and is found to be negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected. Section 72 A of the IT Act, 2000 deals with the breaches of Information and provides for Compensation and punishment for disclosure of Information in breach of Contractual Agreement. Under the provisions, if a person is found guilty, he is liable for imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both. Storing, processing of personal data: The Personal Data Protection Bill, 2019, bars storing and processing of personal data by entities without the explicit consent of an individual.

Data on health can be processed without consent: Data concerning health services and for complying with any law or court orders can be processed without the consent.

Empowers Govt to exempt agencies from the law: The legislation empowers the Central government to exempt government agencies from the application of the Act for "certain" processing of personal data.

Right to Erase data: The bill empowers citizens to have right over their personal data. They can the correct inaccurate data or erase it. They can update or port the data to other fiduciaries and also have a right to restrict or prevent its disclosure. Penalty: The bill provides for a penalty of up to Rs 15 crore or 4 per cent of global turnover for companies

found violating norms under the Personal Data Protection Bill, while in case of certain minor violations, it proposes a penalty of Rs 5 crore or 2 per cent of the global turnover.

India is soon enough expected to pass a Bill i.e. Data Protection Bill, 2019 which will take the shape of a codified law and become an Act as soon as it is passed by the parliament and receives the assent of the President of India. Some of the key highlights of the Bill are:- Therefore, it can be seen that India has taken a step forward to comply with the established International standards and guidelines laid down for Data Data Protection and the Bill is expected to meet the International standards.

Disclaimer: This contribution is only for the purpose of information and knowledge sharing among the clients, associates, professionals, and friends and shall not be treated as a solicitation in any manner or for any other purpose whatsoever. The article does not constitute professional guidance or legal opinion. The views expressed in this article do not necessarily constitute the final option of MAHESHWARI & CO.



Maheshwari & Co
Jyotsna Chaturvedi - Principal Associate



jyotsna@maheshwariandco.com



[Jyotsna Chaturvedi | LinkedIn](#)

Mainland China

How has your country/region enacted specific data privacy legislation?

In the People's Republic of China, the Cyber Security Law of the People's Republic of China (the "CSL") came into effect on 1 June 2017. The CSL imposes data privacy obligations on network operators, which includes most companies involved in any kind of internet-based services. The CSL also regulates critical information infrastructure operators, this encompasses operators of information infrastructure that, if damaged or infiltrated, could threaten national security, national economy, people's livelihood and public interests.

The PRC also has a non-binding Personal Information Security Specification ("PI Specification"), which was drafted with reference to the GDPR. Although not binding, the PI Specification has been used as authority by the PRC Courts when tackling issues of personal data privacy and many companies in the PRC use the PI specification as a guide.

On 21 October 2020, the PRC published a draft of a new legislation called the Personal Information Protection Law ("PIPL"). Furthermore, a draft Data Security Law ("DSL") has been announced and is proposing the implementation of a comprehensive state-directed data security system. Although the PIPL and DSL are yet to be formally introduced, it seems that the CSL, PIPL and the DSL will form the three fundamental security laws in PRC.

How does this compare to GDPR?

The basis on which the CSL was introduced differs from the GDPR. The CSL focuses on national security, cyberspace sovereignty, and the protection of lawful rights and interests, whereas the GDPR aims at the protection of personal data and the regulation of its use. This means that both

sets of legislation approach personal information protection differently. The GDPR approaches it as a critical component of individuals rights, whereas the CSL's data protection measures focus on securing the PRC's network infrastructure and the data that passes through it. Overall, the CSL emphasises, more so than the GDPR, the role of national-level network and data security in protecting individual privacy. Of course, there are many specific differences and similarities between the sets of legislation, but generally speaking both approach data security from different standpoints and the CSL tends to include broader definitions and provisions which are open to more interpretation.

The CSL provides limited extraterritorial application and differs from the GDPR in this respect. However, the draft PIPL proposes extraterritorial application overseas. Like the GDPR, the PIPL proposes that overseas entities and individuals will be caught by its provisions if they process the personal data of data subjects in the PRC. This draft law resembles Article 3(2) of the GDPR and data processors will be caught if they are collecting/processing data for the purposes of selling goods or services and/or profiling customers through analytics.

A stark difference between the CSL and the GDPR, is their coverage of consent. However, the draft PIPL provides that consent must be given, except in circumstances of legitimate interest. It also clarifies the requirements for consent to be deemed as given.

The CSL specifies significant cross-border data transfer restrictions. However, the PIPL attempts to provide a more practical cross-border data transfer legislative framework for organisations to follow. Broadly speaking and subject to various restrictions, it proposes that most organisations will be permitted to access and transfer most personal data outside of the PRC, in various circumstances. Some examples include, if the organisation has obtained

explicit consent from the relevant data subject for the access/transfer and the organisation has undertaken a personal information risk assessment on such access/transfer. Cross-border transfer of personal data to foreign authorities requires Chinese regulators 'prior approval under the draft PIPL, this is also consistent with the DSL.

What was GDPR impact on such legislation?

The PI Specification was drafted with reference to the GDPR, therefore it contains some similarities. Many companies within PRC also use the PI Specification as a basis for their personal information protection rules and regulations. As touched upon, the CSL varies from the GDPR in many ways, however the PIPL signifies a closing of the gap between the GDPR and PRC's data privacy legislations. It seems likely that the GDPR has influenced the areas covered in the new legislation and provided some level of guidance.

Significant examples in your country/region: cases, penalties or breaches

The draft PIPL proposes significant penalties for serious violations, including rectification orders, confiscation of illegal gains, business suspension, revocation of business licenses, and fines of up to RMB50 million (approx. US\$7.6 million) or five percent of turnover in the previous year. Individuals in charge of personal information protection will also be subject to penalties that can be up to RMB1 million (approx. US\$153,200). With regard to CSL, a number of enterprises have been punished for their failure to perform network security protection obligations or for data leakage. In August 2018, many residents of Huazhu, a domestic hotel, had their personal information leaked and sold online. The perpetrators were arrested. In March 2020, Sina Weibo, a domestic social network giant, was interviewed by the National Information Security Standardization Technical Committee for App

data leakage caused by malicious access to user interface.

What are local and international clients' biggest concerns when you are advising about data privacy? What are the main challenges your clients have faced, and which ones will have to face in the future to comply with data privacy legislation?

Before the release of the PIPL, PRC has relied on scattered provisions on personal information protection and various measures from the Cybersecurity Law. Then, PRC gradually built out its data privacy systems through the release of PIPL in May 2018. The release of PIPL was in response to the drastic increase of online frauds and misuse of personal information. However, it is still difficult for citizens to prove violations and seek damages. Besides, the formulation of PIPL and Cybersecurity Law were more 'national security' driven. The current system still lacks clear measures to protection citizens privacy when national security or public interest are invoked.



Hugill & Ip
Carmen Tang - Partner | Data Privacy



carmen.tang@hugillandip.com



[Carmen Tang | LinkedIn](#)



Hugill & Ip
Marco Raccuia - Head of Finance & Operations



marco.raccuia@hugillandip.com



[Marco Raccuia | LinkedIn](#)

Hong Kong

How has your country/region enacted specific data privacy legislation?

In Hong Kong, the Personal Data (Privacy) Ordinance, Laws of Hong Kong, Cap. 486 (PDPO) was passed in 1995 and took effect from December 1996. Its goal is to protect individuals' personal data and it contains 6 core Data Protection Principles (DPPs). These principles give guidance on how data users should collect, handle and use personal data.

How does this compare to GDPR?

Conceptually, the GDPR and PDPO do have similarities, in that they both require protection of data inside a firm and controls on where data is externally distributed, however it may be fair to say that the PDPO does not go as far as the GDPR. Consent for data collection is not a requirement under the PDPO. This is dissimilar to the GDPR which puts a big emphasis on consent for data processing being given by a statement or a clear affirmative action from the data subject. However, the PDPO does require data users to provide notice that data will be taken and if the data is to be used for new purposes, the data user will need the data subject's consent.

Both the PDPO and the GDPR require certain notice requirements, however unlike the GDPR, the PDPO contains no right to erasure, no right to restriction of processing and data portability and no general right to object to processing.

Although under the PDPO data processors are not directly regulated, the PDPO Guidance Notes stipulate that a data processor is required to take the same security measures around the data that the data owner would have to take if they were processing the data themselves.

A noticeable difference between the GDPR and

the PDPO can be seen upon examination of each legislation's definition of "personal data". The GDPR definition has a wider net and catches more forms of data, such as genetic data and biometric data, whereas the PDPO's definition makes no distinction between sensitive and non-sensitive personal data. The two legislations also differ in their approach to breach notifications. If there is a data breach, the GDPR requires users to notify the relevant data protection authority and, in certain circumstances, the data subject themselves. The PDPO recommends breach notifications to the Privacy Commissioner and to data subjects but imposes no mandatory obligation to do so.

When focusing on extra-territorial reach, we can see that the PDPO only applies to data users who are collecting, holding using or processing personal data in or from Hong Kong – the GDPR does not only apply within the EU but also outside.

In terms of businesses and their obligations towards data privacy, the PDPO does not enforce an accountability principle like the GDPR does, but it is advocated by the Privacy Commissioner. The GDPR makes it compulsory to appoint a data protection officer if data processing is conducted by a public body, involves large-scale data monitoring or specifically involves large scale sensitive data. The PDPO merely advises it.

What was GDPR impact on such legislation?

When the PDPO was being drafted, reference was made to the relevant requirements under the OECD Privacy Guidelines 1980 and the EU Directive. This means that the PDPO and the GDPR share various features. However, as touched upon, businesses that are not in violation of the PDPO, may be in violation of the GDPR.

Organizations outside the EU can still be caught by the GDPR if:

I. they offer goods or services to data subjects in the EU;

or

II. monitor the behaviour of data subjects in the EU.

If a business does not blatantly offer goods or services to the EU, it may still be caught by the GDPR if it is apparent that the organisation envisages offering goods or services to, or targets, individuals in the EU. This will depend on the specific situation, but businesses should be careful when setting up their websites for this reason. If languages or EU currency, for example, are used on a company's website this could well be seen as attempting to sell goods and/or services to an EU market and therefore be subject to the GDPR. Businesses may struggle to show that they do not have an intention to sell goods or service to an EU customer base, unless they have clear wording on their website and actively exclude orders from the EU.

If languages or EU currency are used on a company's website this could well be seen as attempting to sell goods and/or services to an EU market and therefore be subject to the GDPR ””

Furthermore, the concept of "monitoring" under the GDPR is very wide, websites using cookies, location tracking apps or other types of web analytics tools may be classified as "monitoring" EU subjects. Again, this is dependent on the facts, but broadly speaking there must be an intention to track and use the data to profile individuals or monitor behavioural trends.

If a business has an "establishment" within the EU

and it processes or holds personal data, it will be regarded as "processing data". An "establishment" can vary, but includes the presence of an office, or appointment of staff in the EU.

Significant examples in your country/region: cases, penalties or breaches

The Privacy Commissioner is empowered to serve enforcement notices on data users, the contravention of which can lead to penalties (following judicial processes) of up to HK\$1 million (US\$128,000) and imprisonment for up to five years. In April 2016, a Community Service Order of 80 hours was imposed on an insurance agent for the offences of (i) using the personal data of a data subject in direct marketing without taking specified actions/obtaining consent; and (ii) failing to inform the data subject, when using his personal data in direct marketing for the first time, of his right to request (without charge) that his personal data not be used in direct marketing. In September 2019, a telecommunications company was fined HK\$84,000 after pleading guilty to 14 charges which related to the offence of failing to comply with the data subject's request to cease using her personal data in direct marketing. This case recorded the highest number of charges and second highest amount of fine since the provisions relating to regulating direct marketing activities came into effect in 2013. The first imposition of a prison sentence for a breach of the PDPO was in December 2014. In this case, a former insurance agent was sentenced to four weeks of imprisonment for offences including two counts of making a false statement to the Privacy Commissioner. It should however be noted that the insurance agent also simultaneously pleaded guilty to other fraud offences and that his sentence for breaching the PDPO arose from his conduct during the Privacy Commissioner's investigation as opposed to for breaching the data protection principles under the PDPO.

What are local and international clients' biggest concerns when you are advising about data privacy? What are the main challenges your clients have faced, and which ones will have to face in the future to comply with data privacy legislation?

Given that most business transactions nowadays require cross-border data transfer, clients would have to address to the gaps in coverage of data protection laws in different jurisdictions. Some countries have already had well established data protection laws while there are still many countries with no relevant legislation. On the other hand, gaps among laws in different countries can create complex problems which may hinder those countries to meet 'adequacy tests' for cross-border transfers, which may result in disputes and complaints. This means client have to be prepared to spend considerable sum on legal fees for the sake of ensuring compliance of laws and regulations in different countries.

Gaps among laws in different countries can create complex problems [...] which may result in disputes and complaints ”

Sometimes, data protection requirements may become compliance burdens for businesses:

- **Registration requirements:** some countries may require data controllers to register their operations or even individual data set with local data protection authority. Processes may be time-consuming and bureaucratic. The registration requirements could hamper the ability of businesses to establish one set of data protection processes for use across all jurisdictions.

- **Requirements to appoint data protection officers:** it seems to be common requirement in national laws is for each business to appoint a specific data protection officer. For large organizations, they may not find it an issue but for small companies it may be a burden. For example, under GDPR, a data protection officer must be independent and an expert in data protection. Small businesses may have to assign staff to attend professional courses to equip the same to become qualified as DPO. Alternatively, they will have to allocate fund to externally appoint such expert which is a burden.



Hugill & Ip
Carmen Tang - Partner | Data Privacy

 carmen.tang@hugillandip.com

 [Carmen Tang | LinkedIn](#)



Hugill & Ip
Marco Raccuia - Head of Finance & Operations

 marco.raccuia@hugillandip.com

 [Marco Raccuia | LinkedIn](#)



Dominican Republic

How has your country/region enacted specific data privacy legislation?

In the Dominican Republic, Law No. 172-13 on Data Protection ("Law 172-13") came into effect on December 15, 2013. It should be noted that this regulation was conceived to regulate specially the personal data managed by the credit bureaus. Therefore, this law has stated general rules on personal data but it does not establish special regulations for the different subjects, such as network operators; who are the ones who evidently handle the greatest amount of personal data.

Moreover, due the impact of the GDPR, the previous Government was preparing a new draft of legislation to include similar provision contained in the GDPR. However, as for today, said draft has not been filed before the National Congress for its discussion.

How does this compare to GDPR?

Law 172-13 is only applicable within the Dominican Republic and does not have any extraterritorial application such as the GDPR. Law 172-13 does recognize the right to access, rectification, cancellation and opposition to personal data as the GDPR, but it does not recognize the right of portability as stated in the GDPR.

Furthermore, pursuant Law 172-13 the treatment and transfer of personal data is illegal when data holder has not given his/her free, express and conscious consent, and it must be in writing or by another means that allows it to be equated, according to the circumstances. In general, this notion of "consent" is similar to what the GDPR provides, nonetheless, the GDPR is more specific on the details regarding

the data holder consent. For instance, GDPR states that when evaluating whether consent has been freely given, the fact that, among other things, the performance of a contract, including the provision of a service, is subject to consent to the processing of personal data, will be taken into account to the greatest extent possible that are not necessary for the execution of said contract.

Moreover, Law 172-13 does not recognize the figure of the "data protection officer" as established in the GDPR. Likewise, the sanctions established in Law 172-13 do not have a general regulatory body that can apply them, apart from the specific sanctions against credit bureaus by the Superintendency of Banks. Another important note is that Law 172-13 does not establish the need to have a "Record of Treatment Activities" as established in the GDPR. In addition, the "right to be forgotten" is neither recognize in Law 172-13. Finally, the need to impose security measures is quite limited, unlike what is established in the GDPR.

Clients are concerned about the scope of application of Law 172-13, especially in terms of territorial application ”

What was GDPR impact on such legislation?

As mentioned above, as Law 172-13 is prior to the GDPR, there has been no real impact. However, there is no doubt that the next amendment to this law will have a significant impact by the GDPR.

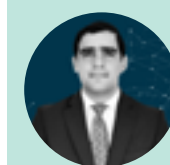
Significant examples in your country/region: cases, penalties or breaches

There have been no significant precedents for cases or penalties for violation of Law 172-13. Mainly,

due to the fact that, as mentioned above, this law has important gaps in terms of the application of sanctions, due to the lack of a general regulatory entity that applies such sanctions. In addition, there is no real culture of personal data protection in the Dominican Republic. Lately, citizens have started to worry a little about their privacy, especially due to the increase in the use of technological platforms due to the Covid-19 pandemic.

What are local and international clients' biggest concerns when you are advising about data privacy? What are the main challenges your clients have faced, and which ones will have to face in the future to comply with data privacy legislation?

In the first place, clients are concerned about the scope of application of Law 172-13, especially in terms of territorial application. Also, the obligations imposed by this legislation, as well as the risks of failing to comply with said obligations. We anticipate that the challenges of the future will be related to the establishment of a regulatory entity that applies the data protection law to all subjects, regardless of the sector of the economy in question. Likewise, the main challenge will be once the current legislation is modified, even clearer rules will be established in relation to the rights of citizens regarding their privacy.



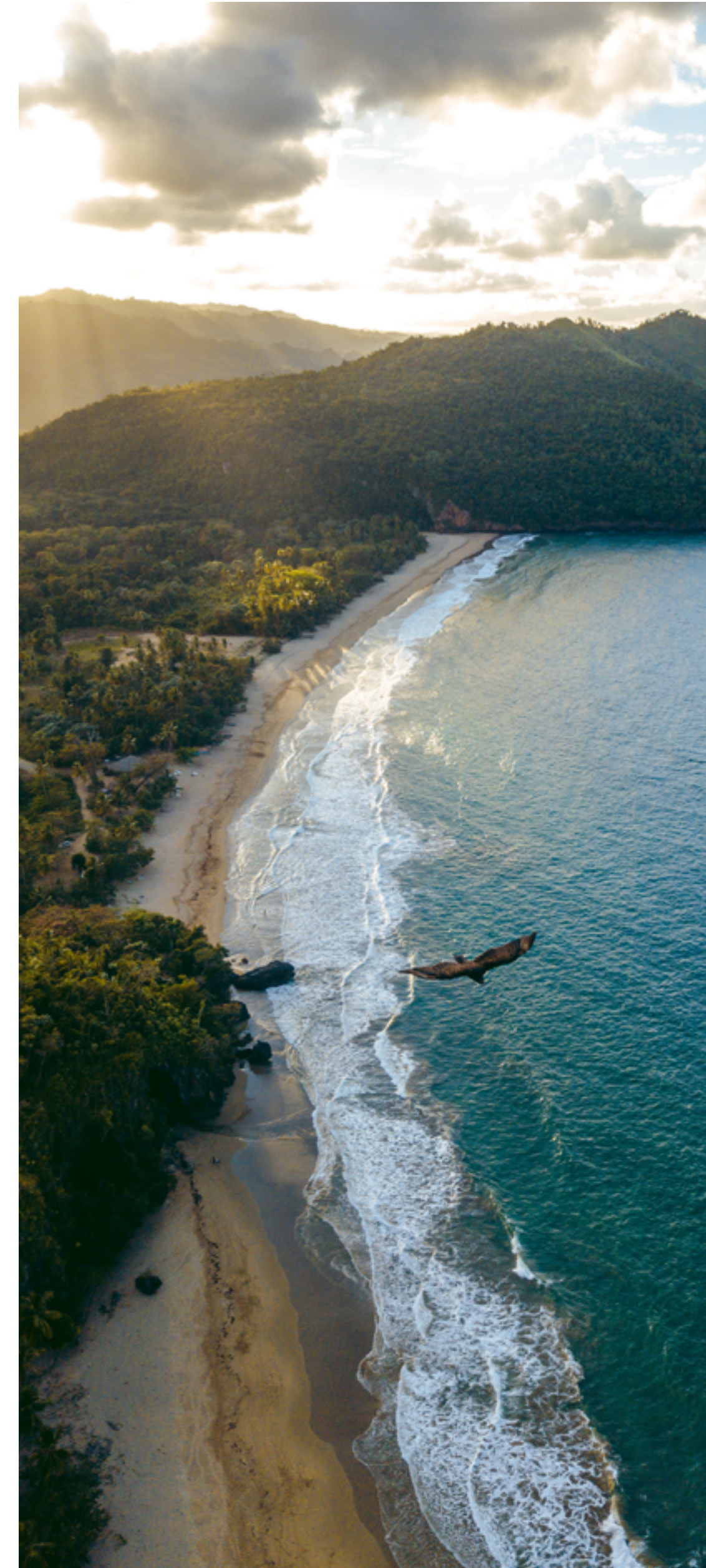
ECIJA
Arístides Victoria Peláez - Associate



avictoria@ecija.com



[Arístides Victoria Peláez](#) | [LinkedIn](#)





Mexico

Federal Law for the Protection of Personal Data held by Private Parties (LFPDPPP).

How has the right to the protection of personal data evolved in Mexico?

In 2009, it was recognized at a constitutional level as a fundamental and autonomous right. In 2010 and 2011, the main and secondary legislation for the private sector was enacted, which establishes the principles and duties that must be observed in the processing of personal data, through the LFPDPPP and its Regulations.

To whom does the LFPDPPP apply?

The LFPDPPP applies to all individuals or legal entities that, in the course of their activities, process personal data, with the exception of credit information entities, and individuals who carry out the processing of personal data for personal use only.

Who is the "responsible" person for the personal data in terms of the LFPDPPP?

The individual or legal entity that decides on the processing of personal data; that is, the one that establishes the purposes of the processing or the use that will be given to the personal data; the type of data that is required; to whom and for what purpose it is shared; how it is obtained, stored and deleted; among other decision factors.

What is an "agent" according to the LFPDPPP?

It is the individual or legal entity that processes personal data according to the instructions of the "responsible". The "agent" is a third party, outside of

the organization of the "responsible".

What is considered "personal data"?

It is any information concerning an identified or identifiable individual. A person is considered identifiable when its identity can be determined through the personal data in question. It is important to consider that if the personal data have been subjected to a dissociation procedure, in such a way that it is not possible to associate them with the owner, or allow its identification, they will no longer be considered as such and, therefore, the regulations will not be applicable.

Clients are often unaware of the legal requirements that must be met in order to exchange or transfer data

What is considered "sensitive personal data"?

They are personal data that affect the most intimate sphere of its owner, or whose misuse may lead to discrimination or entail a serious risk for him/her (e.g.: racial or ethnic origin; health status; religious beliefs; union affiliation; political opinions and sexual preference).

What is not considered "personal data"?

The regulations do not apply to the following information:

- The one related to legal entities;
- The one that refers to individuals in their capacity as traders and professionals; and
- That which refers to individuals and is treated for the purpose of representing the employer or contractor.

What are the main obligations of the "responsible"?

- Implement and disseminate a privacy notice to inform the owners of the treatment that will be given to the personal data, complying with the applicable legal requirements.
- Obtain the consent of the owners for the processing of their personal data, unless an exception applies.
- Establish physical, technical and administrative security measures to guarantee the protection of the personal data.
- Conduct privacy impact assessments to cover the personal data protection risk due to the implementation of new products, services, technologies and business models, as well as to mitigate them.
- Establish internal policies that establish internal guidelines and procedures that must be observed to guarantee the protection of personal data.
- Appoint a department or officer responsible (DPO) for the implementation of the regulations within the organization.

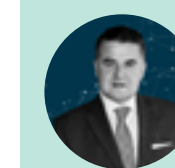
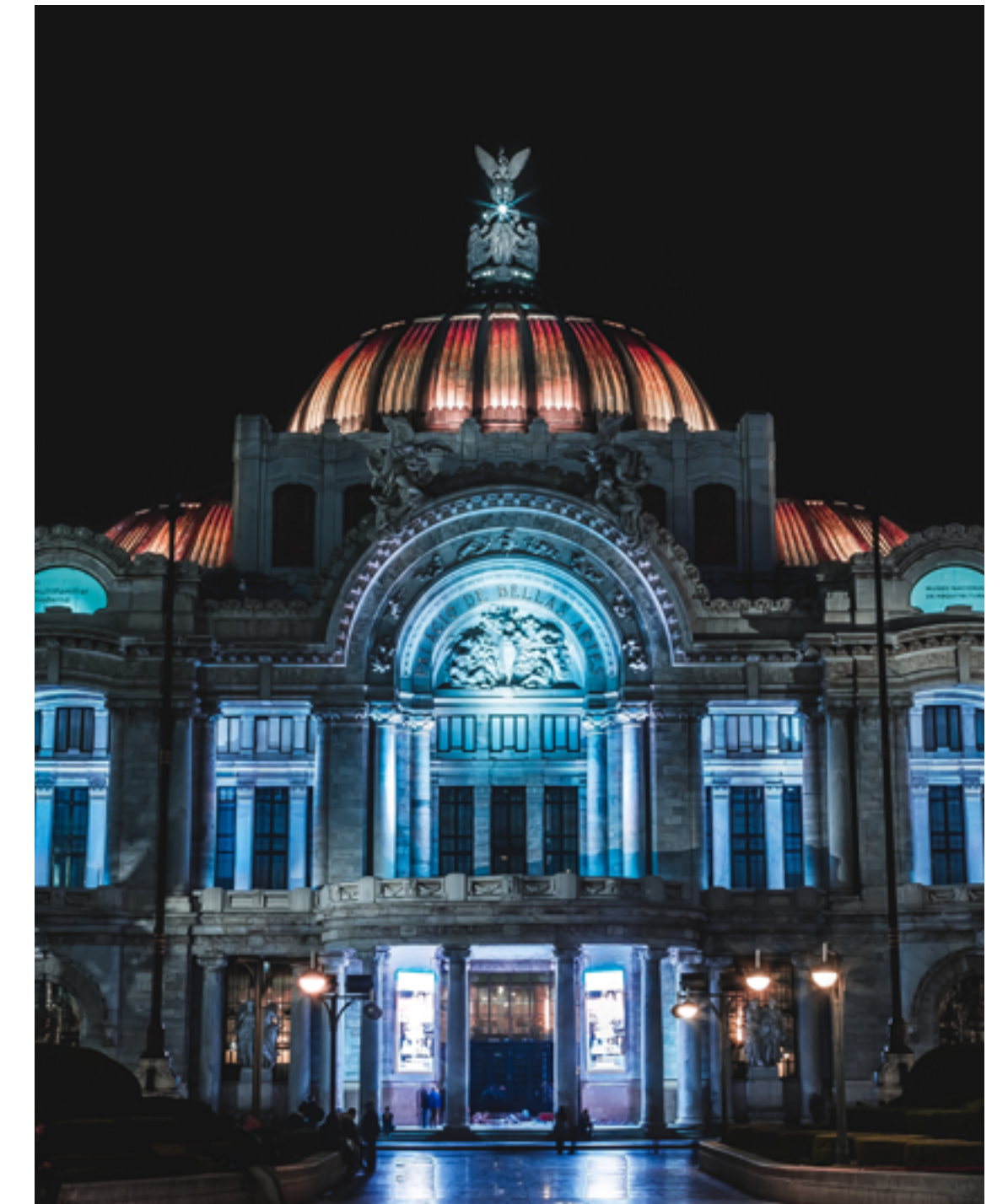
Which are the biggest concerns raised by the clients?

The massive exchange or transfer of personal data is a common practice for various businesses. However, clients are often unaware of the legal requirements that must be met in order to exchange or transfer data, thereby exposing them liability or contingencies.

What are the main challenges that clients have faced in complying with the legislation?

Given that the LFPDPPP is relatively new, thus far there are not enough criteria to determine the way in which companies must comply with their

obligations, that is why on many occasions it is necessary to resort to comparative law.



ECIJA MEXICO, S.C.

Joaquín Rodríguez - Partner, Corporate / M&A, Data Privacy & Compliance



jrodriguezz@ecija.com



[Joaquín Rodríguez | LinkedIn](#)



ECIJA MEXICO, S.C.

Berenice Sagaón - Associate, Data Privacy, Labor & Compliance



bsagaon@ecija.com

United States of America

How has your country/region enacted specific data privacy legislation?

Famously, the U.S. does not have a single, overarching national data privacy law, instead opting for a sector-by-sector approach (e.g., health-related information, financial information). Accordingly, it has been left to the states to enact their own data privacy laws. In this regard, California has led the way with its 2018 California Consumer Privacy Act, extended in 2020 by the California Privacy Rights Act. Other states are following suit.

The U.S. does not have a single, overarching national data privacy law, instead opting for a sector-by-sector approach”

How does this compare to GDPR?

Increasingly, U.S. states are modelling their data privacy legislation on the GDPR. For example, the CCPA/CPRA has very many similarities to the GDPR, adopting a similarly broad definition of "personal information." Some areas of dissimilarity are exemptions under the CCPA/CPRA for information regulated in other ways (e.g., health and financial information), as well as not-for-profit organizations, which remain outside the scope of the law.

What was GDPR's impact on such legislation?

As noted above, U.S. states have looked to the GDPR as a starting point in drafting their own data privacy

legislation, and there is no sense that this will change in the future.

Significant examples in your country/region: cases, penalties or breaches

As of yet, there have been few cases resolved or penalties imposed under the CCPA. Most significant privacy/information security related cases and fines have been at the national level, either via class-action lawsuits or regulatory actions taken by the Federal Trade Commission or the Department of Health and Human Services.

What are local and international clients' biggest concerns when you are advising about data privacy? What are the main challenges your clients have faced, and which ones will have to face in the future to comply with data privacy legislation?

Our clients often have to be convinced that applicable data privacy legislation actually applies to their business! We find ourselves explaining that the "traditional" definition of "personally identifiable information" has now expanded, sweeping in information that may not, particularly to a layperson, seem at first glance to be protectible.

Another big challenge in the U.S. is the absence of a single federal data privacy law. As noted above, until now, the U.S. has taken a sectoral approach to data protection at the federal level, leaving it to states to enact their own separate data privacy laws. As you might expect, this makes compliance much more challenging, as businesses will often find themselves having to comply with different laws based on where they're located and where they do business. Of course, because of California's size and importance, and the reach of the CCPA/CPRA, it is a defensible approach to take that

legislation as the U.S.'s de facto data privacy law, at least until (if?) the U.S. ever enacts a single federal law.

Our clients often have to be convinced that applicable data privacy legislation actually applies to their business”



Trusted Counsel
Evelyn Ashley - Partner



eashley@trusted-counsel.com



[Evelyn Ashley | LinkedIn](#)



California

THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA) AND THE CALIFORNIA CONSUMER RIGHTS ACT (CPRA)



Background

CCPA

On June 28, 2018, the State of California enacted Assembly Bill 375, the California Consumer Privacy Act (CCPA). The CCPA entered into effect on January 1, 2020 and is based on the principles that California consumers should have the ability to control their personal information collected online and that there should be certain safeguards against the misuse of their personal information. Subsequently, several states have followed California's lead and have introduced tougher data privacy legislation of their own, including Virginia, New York, Massachusetts, Washington, and Texas. California has long been a leader in the United States for privacy and data security regulation – the state enacted its first breach notification law in 2003. The CCPA is a bold

step for data privacy in the United States, following closely on the European Union's General Data Protection Regulation (GDPR), similar legislation that went into effect on May 25, 2018.

CPRA

The California Privacy Rights Act of 2020 (CPRA) was approved by a majority of California voters as a ballot initiative on November 3, 2020 and will become effective on January 1, 2023 with respect to personal information collected on or after January 1, 2022. The CPRA builds on, expands and, in some cases, actually limits the scope of, the CCPA. The key features of the CPRA (and differences from the CCPA) will be discussed in greater detail below.

CCPA

To which businesses does the CCPA apply?

The CCPA applies to businesses that process the personal information of California residents (called “consumers” in the CCPA) that fall into any of the following three categories:

- Has annual revenues over **USD \$25 million OR**
- Annually receives, directly or indirectly, the personal information of 50,000 or more California **residents, households or devices OR**
- **50% or more** of its annual revenue is derived from **selling** the personal information of California residents

The CCPA does not apply to nonprofit or governmental entities. It also does not apply to for-profit entities that are subject to regulation under certain U.S. federal laws, such as healthcare-related companies and financial services companies.

What is a “service provider” under the CCPA?

The CCPA distinguishes between a “business” and a “service provider.” A service provider is defined as an entity that processes personal information on behalf of a business which has disclosed that personal information to the service provider for a business purpose pursuant to a written contract. That contract must prohibit the service provider from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, or as otherwise permitted by the CCPA. Specifically, the service provider may not retain, use, or disclose the personal information for a commercial purpose other than providing the services specified in the contract with the business.

What is “personal information” under the CCPA?

The CCPA defines personal information broadly as information that identifies, relates to, or could reasonably be linked with a consumer or a consumer’s household. For example, it could include a consumer’s name, social security number, email address, records of products purchased, internet browsing history, geolocation data, fingerprints, and inferences from other personal information that could create a profile about the consumer’s preferences and characteristics.

What is NOT “personal information” under the CCPA?

Personal information does not include publicly available information drawn from federal, state, or local government records. It also does not include deidentified or aggregated consumer data.

What notices are required under the CCPA?

The CCPA requires businesses to provide consumers with certain information in a “notice at collection.” A notice at collection must list the categories of personal information businesses collect about consumers and the purposes for which they use the categories of information. If the business sells consumers’ personal information, then the notice at collection must include a “Do Not Sell” link (discussed further below). The notice must also contain a link to the business’s privacy policy, where consumers can get a more detailed description of the business’s privacy practices and of their privacy rights.

The notice must be provided at or before the point the business collects the personal information. Examples might include a link to the notice at collection on a website’s homepage or on a webpage where a consumer places an order or enters personal information for another reason.

On a mobile app, the notice might be linked in the settings menu.

What rights do consumers have under the CCPA?

Under the CCPA, for the first time in U.S. privacy law, consumers have the right:

- To know all personal information a business has collected about them in the previous 12 months, twice a year and free of charge
- To opt out of the sale of their personal information
- To request deletion of their personal information
- To not be discriminated against if the consumer opts out of the sale of their personal information (any contractual waiver of this right would be deemed to be unenforceable)
- To know the categories of personal information that will be collected about them **before or at the point of** collection, as well as to be notified of any changes to the foregoing
- To know the categories of third parties with whom their personal information is shared
- To know the categories of sources from which their personal information was collected
- To know the business or commercial purpose of collecting their personal information

What is the right to opt-out of sale of personal information?

As noted above, a consumer may request that businesses stop selling their personal information (“opt-out”). With some exceptions, businesses cannot sell a consumer’s personal information after they receive the consumer’s opt-out request unless the consumer later provides authorization once again allowing them to do so. After a consumer has opted out, a business must wait at least 12 months before asking the consumer to opt back in.

How may consumers submit requests under the CCPA?

Businesses must designate at least two methods for consumers to submit their requests—for example, an email address and a website form. One of those methods has to be a toll-free phone number and, if the business has a website, one of those methods has to be through its website. However, if a business operates exclusively online, it only needs to provide an email address for submitting requests.

Businesses cannot force consumers to create an account just to submit a request, but if the consumer already has an account with the business, the consumer may be required to submit the request through that account.

How long does a business have to respond to a consumer request?

Businesses must respond within 45 calendar days, which can be extended by another 45 days (90 days total) if they notify the consumer.

What is the “Do Not Sell My Personal Information” link?

Businesses that sell personal information are subject to the CCPA’s requirement to provide a clear and conspicuous “Do Not Sell My Personal Information” link on their website that allows a consumer to submit an opt-out request. In addition, businesses cannot require consumers to create an account in order to submit their request.

What about children’s personal information?

Businesses can only sell the personal information of a child that they know to be under the age of 16 if they get affirmative authorization (“opt-in”) for the sale of the child’s personal information. For children under the age of 13, that opt-in must come from the child’s parent or guardian. For children who are at

least 13 years old but under the age of 16, the opt-in can come from the child.

How may a business verify that the consumer making a request is who they say they are?

For opt-out requests, businesses are not required to verify that the person submitting an opt-out request is really the consumer for whom the business has personal information, but it may still be advisable for them to ask the consumer for additional information to make sure they stop selling the right person's personal information. If the business asks for personal information to verify a consumer's identity, it can only use that information for this verification purpose.

For **requests to know** and **requests to delete**, businesses must verify that the person making the request is the consumer about whom the business has personal information and may therefore ask the consumer for additional information for verification purposes. As with all other verification-related information, if the business asks for personal information to verify a consumer's identity, it can only use that information for this verification purpose.

How may a service provider (as opposed to a business) respond to a consumer request?

The CCPA does not require (or indeed authorize) a service provider to fulfill a consumer request. It is the business that is responsible for responding to consumer requests. Accordingly, if a consumer submits a request to opt-out to a service provider instead of the business itself, the service provider may deny the request.

If a service provider responds to the consumer request by stating that it will not act on the request

because it is a service provider, the consumer may request the service provider for the identity of the business, but the service provider is not obligated to provide that information.

May a business deny a consumer request?

Yes. If the business cannot verify the consumer's identity, it may (and in cases of requests to delete, must) deny the request. It may also deny the request for certain specified reasons, including:

- The request is manifestly unfounded or excessive, or the business has already provided personal information to the consumer more than twice in a 12-month period
- The information is required to complete a consumer transaction, provide a reasonably anticipated product or service, or for certain warranty and product recall purposes
- The information is required for certain business security practices
- The information is required for certain internal uses that are compatible with reasonable consumer expectations or the context in which the information was provided
- The personal information includes certain sensitive information, such as social security number, financial account number, or account passwords (but the business must still tell the consumer if it's collecting that type of information)
- Disclosure would restrict the business's ability to comply with legal obligations, exercise legal claims or rights, or defend legal claims

How is the CCPA enforced? What rights does a consumer have to sue a business?

Consumers cannot sue businesses for most CCPA violations. A consumer can only sue a business under the CCPA if there is a data breach, and even

then, only under limited circumstances. However, class actions are expressly permitted under the CCPA.

A consumer can sue a business if the consumer's nonencrypted and nonredacted personal information was disclosed in a data breach as a result of the business's failure to maintain reasonable security procedures and practices to protect it. A consumer has the option of suing for monetary damages in an amount actually suffered from the breach or for "statutory damages" of up to \$750 per incident. If a consumer opts to sue for statutory damages, the business must be given written notice of which CCPA sections it violated and 30 days to give the consumer a written statement that it has cured the cited violation(s) and that no further violation(s) will occur. A consumer cannot sue for statutory damages if the business is able to cure the violation and provides a written statement that it has done so, unless the business continues to violate the CCPA contrary to its statement.

Note, however, that the data breach must have involved personal information that was not redacted or encrypted and must have included a consumer's first name (or first initial) and last name in combination with any of the following:

- The consumer's social security number
- The consumer's driver's license number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to identify a person's identity
- The consumer's financial account number, credit card number, or debit card number if combined with any required security code, access code, or password that would allow someone access to a consumer's account
- The consumer's medical or health insurance information

- The consumer's fingerprint, retina or iris image, or other unique biometric data used to identify a person's identity (but not including photographs unless used or stored for facial recognition purposes)

For all violations of the CCPA that do not involve a data breach as described above, only the California Attorney General has jurisdiction to file an action for noncompliance. If notified of noncompliance by the Attorney General, businesses have no more than 30 days to come into compliance in order to avoid civil penalties of up to \$2,500 per violation and \$7,500 per intentional violation.

Of course, as with any regulatory fine or data breach, the reputational harm and brand damage that could result from noncompliance may be incalculable.

CPRA

The CPRA makes the following major changes and enhancements to the CCPA:

- Modifies the definition of "business"
- Creates a new category of "sensitive" personal information
- Creates the California Privacy Protection Agency (CPPA)
- Expands private right of action for security breaches involving personal information
- Sunsets the CCPA's exception for employee personal information and business-to-business personal information on January 1, 2023
- Introduces an overarching purpose limitation obligation with respect to the collection and use of personal information, requiring a business to collect, use, retain and share a consumer's personal information only as "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected"
- Establishes several new consumer rights
- Simplifies and eliminates exceptions to the right to delete
- Broadens the "do not sell" opt-out requirement to include "sharing" of personal information for cross-context/third party advertising
- Requires businesses to honor a consumer's opt-out preference signal
- Institutes a new set of required service provider contract provisions
- Adds an independent and express obligation for businesses to implement "reasonable" security procedures and practices

- Requires certain "high risk" businesses to perform annual cybersecurity audits and to submit to the CPPA risk assessments

How does the CPRA modify the definition of "business"?

Until the CPRA becomes fully effective on January 1, 2023, the CCPA's definition of "business" will remain in place. After January 1, 2023, the CPRA will narrow the application of the definition of "business" in the following ways:

- A business must have had \$25M in annual gross revenues as of January 1 of the preceding calendar year OR
- Buy, sell or share the personal information of at least 100,000 California consumers or households (i.e., "devices" has been deleted) OR
- derives from 50% or more of its revenues from selling or sharing personal information.

The practical importance of these changes is that many online businesses (in particular) that were swept in under the CCPA via the "50,000 devices" threshold will no longer be a "business" subject to the CPRA as of January 1, 2023.

How does the CPRA define "sensitive" personal information?

The CPRA defines "sensitive" personal information as personal information that discloses:

- A consumer's social security, driver's license, state identification card, or passport number
- A consumer's account log-in, financial account, debit card or credit card number combined with any required security or access code, password or credentials allowing access to an account
- A consumer's precise geolocation
- A consumer's racial or ethnic origin, religious or philosophical beliefs or union membership

- The contents of a consumer's physical mail, email and text messages, unless the business is the intended recipient of the communication
- A consumer's genetic data, including:
- Biometric information processed for the purpose of uniquely identifying a consumer
- Personal information collected and analyzed concerning a consumer's health
- Personal information collected and analyzed concerning a consumer's sex life or sexual orientation

What additional obligations does the CPRA impose with respect to sensitive personal information?

- **Additional notice requirements.** The CPRA requires businesses to provide separate disclosures regarding collection of sensitive personal information in its notice to consumers "at or before the point of collection", including the purpose for collection and use, and whether such information is sold or shared. Businesses must not collect additional categories of sensitive personal information or use sensitive personal information collected for additional purposes that are "incompatible" with the disclosed purpose for which the sensitive personal information was collected without first providing the consumer with notice.

- **Right to limit disclosure or use:**

- The CPRA provides consumers a new right to instruct a business to limit its use of the consumer's sensitive personal information to use that is necessary to perform the services or provide the goods reasonably expected by the consumer. If the business uses or discloses sensitive personal information for other purposes, the business must notify the consumer and provide them the right to limit its use and/or disclosure.

- Businesses must create a "Limit the Use of My Sensitive Personal Information" link on its

user interface or a combined sensitive personal information, sale and sharing opt-out link. The business has the alternative of honoring a consumer's opt-out preference signals.

- These obligations must be passed down to service providers and contractors via contractual terms. Service providers and contractors are also required to comply with these obligations after receiving instructions from the business.

- As with the "opt out" right, a business must wait at least 12 months after a consumer instructs the business to limit the use or disclosure of their sensitive personal information before requesting that the consumer authorize such use and disclosure for additional purposes.

What new rights are provided to consumers under the CPRA?

In addition to the right to limit use and disclosure of sensitive personal information discussed above, the CPRA also now gives consumer the right to request correction of inaccurate personal information, the right to opt out of the "sharing" (not just the sale" of personal information, and the right to opt out of automated decision-making technology.

Does the CPRA make any changes to a consumer's right to sue for a data breach?

Yes. The CPRA adds an email address in combination with a password or security question plus answer to the list of data elements that, if breached, could give rise to a private right of action. Note, however, that this private right of action will only apply to breaches of online account credentials that include an email address, not all kinds of online account credentials.

an email address in combination with a password or security question plus answer



How does the CPRA expand the CCPA's "notice at collection" requirements?

The CPRA expands the CCPA's notice requirements for businesses to include the following additional disclosures:

- Whether the consumer's personal information is sold or shared
- How long the business intends to retain each category of personal information or the criteria it will use to determine how long it will retain such information
- If "sensitive" personal information is collected, an independent disclosure identifying the categories of information collected, the purpose each category is collected, and whether such information is sold or shared

Significant here is the codification for the first time of a requirement that businesses not retain personal information for any longer than is necessary to fulfill the purpose for which it was collected.

The CPRA also appears to require a business that is acting only as a third party controlling the collection of personal information to provide notice of such collection to the consumer. It is likely that regulations to be issued by the CPPA will clarify this requirement.

What additional requirements for supplier contracts does the CPRA impose?

The CPRA sets forth certain minimum requirements that must be met in order for a supplier to qualify either as a "service provider" or a "contractor". These categories are important, because a "service provider" or a "contractor" may process personal information disclosed to it by a business without being required to provide notice and opt-out for sales and sharing.

To qualify a supplier as a "service provider" or "contractor," a business must require the supplier to sign a written contract that complies with the following requirements:

For a "service provider", the contract must prohibit the supplier from:

- Selling or sharing the personal information
 - Retaining, using, or disclosing the personal information other than for business purposes specified in the contract or as otherwise permitted by the CPRA
 - Retaining, using, or disclosing the information outside of the direct business relationship between the business and the supplier
 - Combining the personal information received from or on behalf of the business with personal information received or collected in other contexts
- For a "contractor", the contract must prohibit the supplier from:
- Selling or sharing the personal information
 - Retaining, using, or disclosing the personal information other than for business purposes specified in the contract or as otherwise permitted by the CPRA
 - Retaining, using, or disclosing the information outside of the direct business relationship between the business and the supplier
 - Combining the personal information received from or on behalf of the business with personal information received or collected in other contexts

AND

The contractor must certify that it understands these requirements and will comply with them.

Additionally, a contract with a contractor must allow the business to monitor the contractor's compliance with the contract at least once every

twelve (12) months.

Finally, the CPRA also mandates new minimum contractual provisions whenever a business "sells" personal information to a third party, "shares" it for behavioral advertising purposes or otherwise discloses it for a "business purpose" to a service provider or contractor. For each of these use cases, the applicable contract should:

- Specify the information is sold or disclosed only for limited and specified purposes
- Obligate the contracting party to comply with the CPRA and provide the same degree of privacy protection as that required by the CPRA
- Require the contracting party to notify the business if it can no longer meet its obligations under the CPRA
- Authorize the business to take "reasonable and appropriate steps" to ensure the contracting party uses the personal information in a manner consistent with the CPRA or to cease and remediate unauthorized use of personal information

How does the CPRA change businesses' (and service providers') information security obligations?

In a departure from the CCPA, the CPRA imposes an affirmative obligation on certain businesses to implement "reasonable" security procedures and practices to protect consumers' personal information. The CPRA also requires businesses to obtain contractual commitments from certain third parties that they will provide the same level of information security with respect to the personal information that they process as that required by businesses themselves. In addition, the CPRA imposes a new requirement of annual cybersecurity audits for businesses whose processing of personal information presents a significant risk to consumers' privacy or security. These same businesses will also be required to submit risk assessments of how

they process personal information, balancing the business benefits of processing the information against the potential risks to consumer rights. It is currently unresolved exactly which businesses will be subject to these new audit and risk assessment requirements, but the criteria will include the size and complexity of the businesses and the nature and scope of their processing activities.

What are the roles and responsibilities of the new California Privacy Protection Agency?

Under the CPRA, responsibility for regulation, implementation and enforcement of the CCPA/CPRA has been transferred from the California Attorney General to a new agency, the California Privacy Protection Agency (CPPA). The CPPA will be managed by a five-person board comprised of experts in privacy and technology.

One of the most important duties of the CPPA will be to draft regulations implementing many of the provisions of the CPPA. By the later of July 1, 2021, or six months after the CPPA notifies the Attorney General that it is ready to begin the process of drafting regulations, the CPPA will officially assume this responsibility, and final regulations must be adopted by July 1, 2022.

The other primary duty of the CPPA will be enforcement of the CCPA/CPRA. Following an investigation and administrative hearing, if the CPPA finds that a violation has occurred, the CPPA may order a business to cease the violation and/or impose a fine of \$2500 per violation or \$7500 per intentional violation or per violation involving the personal information of minors. Note, however, that the CPRA does not strip the California Attorney General of his or her enforcement authority, and the Attorney General retains concurrent jurisdiction to investigate violations of the CCPA/CPRA and impose fines (in the same amounts as the CPPA). But if the

CPPA has already issued a decision or order, the Attorney General may not then file a civil action for the same violation.

What other changes does the CPRA make to enforcement?

The CPRA imposes higher administrative and civil penalties for violations involving the personal information of children and minors. The CPPA or the California Attorney General may seek penalties of up to \$7,500 for each violation of the CPRA involving a consumer under the age of 16.

What are the key dates for implementation of the CPRA?

December 2020:

CPRA becomes "preliminarily" effective, and the California Attorney General begins process of transferring regulatory authority to CPPA

July 1, 2021:

Beginning on the later of this date or six months after the CPPA provides notice that it is ready to begin rulemaking, the California Attorney General will transfer authority to the CPPA to adopt regulations under the CPRA

January 1, 2022:

Personal information collected by businesses becomes subject to obligations under the CPRA.

July 1, 2022:

Final CPRA regulations must be adopted

January 1, 2023:

CPRA becomes fully operationally effective

July 1, 2023:

CPPA will begin enforcing the CPRA with respect to violations occurring on or after this date



Trusted Counsel
Evelyn Ashley - Partner



eashley@trusted-counsel.com



[Evelyn Ashley | LinkedIn](#)



Interact Law



Our Global Network

Denmark

[Advodan](#)

Nigeria

[AEC legal](#)

Portugal

[Antas da Cunha Ecija](#)

Poland

[B2Rlaw](#)

England

[BDB Pitmans](#)

Morocco, Algeria, Tunesia, Côte d'Ivoire

[Bennani & Associés](#)

Romania, Hungary, Bulgaria, Czech Republic, Croatia, Slovakia

[CEE Attorneys](#)

France

[Cohen Amir-Aslani](#)

The Netherlands

[De Vos & Partners Advocaten](#)

Spain

[ECIJA Spain](#)

Costa Rica, Dominican republic, El Salvador, Guatemala, Honduras, Nicaragua

[ECIJA Central America & Caribbean](#)

Mexico

[Ecija Mexico](#)

Ecuador

[Ecija - GPA Abogados](#)

Chile

[Ecija Otero](#)

Peru

[Estudio Muniz](#)

Belgium

[Everest Law](#)

Hongkong - China

[Hugill & Ip](#)

Germany

[ljh Lindlbauer PartmbB](#)

Scotland

[MacRoberts LLP](#)

India

[Maheshwari & Co](#)

Zambia

[P.H.Yangailo](#)

Greece

[Politis & Partners](#)

Italy, Romania, Albania, Serbia

[Tonucci & Partners](#)

Luxemburg

[Van Den Bulke](#)

Switzerland

[Wenger & Vieli](#)

USA

[Westerman Ball Ederer Miller Zucker & Sharfstein, LLP](#)

Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines Singapore, Thailand and Vietnam

[Zico Law](#)