SLOVAK REPUBLIC

# Data Protection Laws of the World

DLA PIPER

# Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. As we step into 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

## Europe

Established data protection laws in Europe continue to evolve through active regulatory guidance and enforcement action. In the United Kingdom, the UK government has proposed reforms to data protection and e-privacy laws through the new Data (Use and Access) Bill ("**DUAB**"). The DUAB follows the previous government's unsuccessful attempts to reform these laws post-Brexit, which led to the abandonment of the Data Protection and Digital Information (No.2) Bill ("**DPDI Bill**"), in the run-up to the general election. Although the DUAB comes with some bold statements from the government that it will *"unlock the power of data to grow the economy and improve people's lives"*, the proposals represent incremental reform, rather than radical change.

## United States

In the United States, legislation on the federal and in particular state level continues to evolve at a rapid pace. Currently, the US has fourteen states with comprehensive data privacy laws in effect and six state laws will take effect in 2025 and early 2026. Additionally, at the federal level, the new administration has signaled a shift in enforcement priorities concerning data privacy. Notably, there is a renewed focus on the regulation of artificial intelligence (AI), with an emphasis on steering away from regulation and promoting innovation. This includes the revocation of previous executive orders related to AI and the implementation of new directives to guide AI development and use.

In the realm of children's privacy, many of the new administration's supporters in Congress have indicated a desire to make the protection of children on social media a top priority, and new leadership at the Federal Trade Commission (FTC) appears aligned on this goal, albeit with a willingness to take another look at the recently adopted amendments to the Children's Online Privacy Protection Act (COPPA) Rule. Health data

privacy remains a critical concern, with a handful of states following Washington state's lead in enhancing or adopting health data privacy laws. On the international data transfer front, Executive Order (E.O.) 14117 " Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" as supplemented by the DOJ's final Rule will impact companies transferring data into certain jurisdictions, such as China, Iran and Russia. Another area of focus for companies with an EU presence will be the Trump administration's approach to the Privacy and Civil Liberties Oversight Board, as it is a critical pillar of the EU/UK/Swiss-US Data Privacy Framework.

## Asia, the Middle East, and Africa

Nowhere is the data protection landscape changing faster – and more fundamentally – than in Asia, with new laws in India, Indonesia, Australia and Saudi Arabia, as well continued new data laws and regulations in China and Vietnam. The ever-evolving data laws, as well as the trend towards regulating broader data categories (beyond personal data), in these regions continue to raise compliance challenges for multi-national businesses.

## Emerging trends in data governance

Unlocking data, regulating the relentless advance of AI, creating fairer digital markets and safeguarding critical infrastructure against the ever growing cyber threat, continue to impact and overlap with the world of data protection and privacy. Perhaps most notably, the EU have introduced a raft of new laws forming part of its ambitious digital decade, which will bring huge change to businesses operating within the EU. With the rapid adoption of artificial intelligence enabled solutions and functionality, data protection supervisory authorities have been closely scrutinising the operation of AI technologies and their alignment with privacy and data protection laws. For businesses, this highlights the need to integrate date protection compliance into the core design and functionality of their AI systems. In the midst of this, the privacy community found itself at the centre of an emerging debate about the concept of 'AI governance'. This is not a surprising development – AI systems are creatures of data and the principle-based framework for the lawful use of personal data that sits at the heart of data protection law offers a strong starting point for considering how to approach the safe and ethical use of AI. As AI technologies advance, so will regulatory expectations. It is expected that regulatory scrutiny and activity will continue to escalate and accelerate in tandem with the increase in integration of powerful AI models into existing services to enrich data. Whilst privacy professionals cannot tackle the AI challenge alone, expect them to continue to be on the front lines throughout 2025 and beyond.

## Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

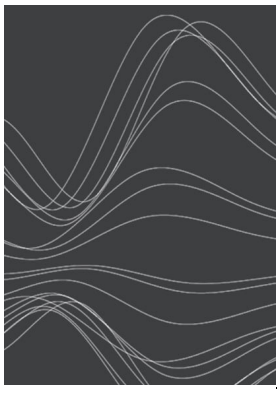
## Africa key contact

**Monique Jefferson**
Director
monique.jefferson@dlapiper.com
Full bio

## Americas key contact

**Andrew Serwin**
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

## Asia Pacific key contact



**Carolyn Bigg**
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

## Europe key contacts

**Andrew Dyson**
Partner
andrew.dyson@dlapiper.com
Full bio

**Ewa Kurowska-Tober**
Partner
Head of Intellectual Property and Technology, Poland
ewa.kurowska-tober@dlapiper.com
Full bio

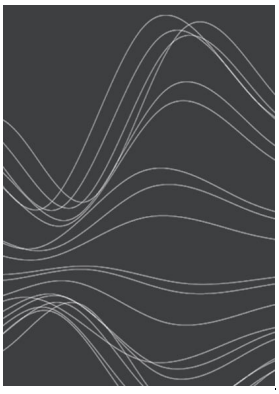
**John Magee**
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

## Middle East key contact

**Rami Zayat**
Partner
rami.zayat@dlapiper.com
Full bio

## Editors

**Kate Lucente**
Partner
kate.lucente@us.dlapiper.com
Full bio



**Lea Lurquin**
Associate
lea.lurquin@us.dlapiper.com
Full bio

# Slovak Republic

LAST MODIFIED 17 JANUARY 2024

## Data protection laws

### EU regulation

The General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**) is a European Union law which entered into force in 2016 and, following a two year transition period, became directly applicable law in all Member States of the European Union on 25 May 2018, without requiring implementation by the EU Member States through national law.

A 'Regulation' (unlike the Directive which it replaced) is directly applicable and has consistent effect in all Member States. However, there remain more than 50 areas covered by GDPR where Member States are permitted to legislate differently in their own domestic data protection laws, and there continues to be room for different interpretation and enforcement practices among the Member States.

#### Territorial Scope

Primarily, the application of the GDPR turns on whether an organization is established in the EU. An 'establishment' may take a wide variety of forms, and is not necessarily a legal entity registered in an EU Member State.

However, the GDPR also has extra-territorial effect. An organization that it is not established within the EU will still be subject to the GDPR if it processes personal data of data subjects who are in the Union where the processing activities are related "*to the offering of goods or services*" (Article 3(2)(a)) (no payment is required) to such data subjects in the EU or "*the monitoring of their behaviour*" (Article 3(2)(b)) as far as their behaviour takes place within the EU.

---

### Slovak Republic regulation

As a member of the European Union, Slovakia is bound by the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection

of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (the "**GDPR**").

Furthermore, Slovakia adopted Act No. 18/2018 Coll. on the protection of personal data and on amending and supplementing certain acts (the "**Slovak Data Protection Act**") implementing the GDPR, which became effective as of 25 May 2018.

## Definitions

### EU regulation

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 4). A low bar is set for "*identifiable*" – if the natural person can be identified using "all means reasonably likely to be used" (Recital 26) the information is personal data. A name is not necessary either – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person.

Online identifiers are expressly called out in Recital 30, with IP addresses, cookies and RFID tags all listed as examples.

The GDPR creates more restrictive rules for the processing of "**special categories**" (Article 9) of personal data (including data relating to race, religion, sexual life, data pertaining to health, genetics and biometrics) and personal data relating to **criminal convictions and offences** (Article 10).

The GDPR is concerned with the "**processing**" of personal data. Processing has an extremely wide meaning, and includes any set of operations performed on data, including the mere storage, hosting, consultation or deletion of the data.

Personal data may be processed by either a "**controller**" or a "**processor**". The controller is the decision maker, the person who "*alone or jointly with others, determines the purposes and means of the processing of personal data*" (Article 4). The processor "*processes personal data on behalf of the controller*", acting on the instructions of the controller. In contrast to the previous law, the GDPR imposes direct obligations on both the controller and the processor, although fewer obligations are imposed on the processor.

The "**data subject**" is a living, natural person whose personal data are processed by either a controller or a processor.

### Slovak Republic regulation

The definitions provided by the GDPR apply.

### EU regulation

## National data protection authority

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (similar to the CNIL in France or the ICO in the UK). The European Data Protection Board (the replacement for the so-called Article 29 Working Party) is comprised of delegates from the supervisory authorities, and monitors the application of the GDPR across the EU, issuing guidelines to encourage consistent interpretation of the GDPR.

The GDPR creates the concept of "**lead supervisory authority**." Where there is cross-border processing of personal data (i.e. processing taking place in establishments of a controller or processor in multiple Member States, or taking place in a single establishment of a controller or processor but affecting data subjects in multiple Member States), then the starting point for enforcement is that controllers and processors are regulated by, and answer to, the supervisory authority for their main or single establishment, the so-called "lead supervisory authority."

However, the lead supervisory authority is required to cooperate with all other concerned authorities, and a supervisory authority in another Member State may enforce where infringements occur on its territory or substantially affect data subjects only in its territory. The concept of lead supervisory authority is therefore of somewhat limited use to multinationals.

### Slovak Republic regulation

The Data Protection Office of the Slovak Republic (the 'Slovak Office') is:

*Úrad na ochranu osobných údajov Slovenskej republiky* (Official Slovak Name)

*Hraničná* 12
820 07, *Bratislava* 27
Slovak Republic

The Slovak Office is the supervisory authority and is responsible for overseeing the Slovak Data Protection Act and the GDPR in Slovakia.

## Registration

### EU regulation

There are no EU-wide systems of registration or notification and Recital 89 of the GDPR seeks to prohibit indiscriminate general notification obligations. However, Member States may impose notification obligations for specific activities (e.g. processing of personal data relating to criminal convictions and offences). The requirement to consult the supervisory authority in certain cases following a data protection impact assessment (Article 36) constitutes a notification requirement. In addition, each controller or processor must communicate the details of its data protection officer (where it is required to appoint one) to its supervisory authority (Article 37(7)).

In many ways, external accountability to supervisory authorities via registration or notification is superseded in the GDPR by rigorous demands for internal

accountability. In particular, controllers and processors are required to complete and maintain comprehensive records of their data processing activities (Article 30), which must contain specific details about personal data processing carried out within an organisation and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

## Slovak Republic regulation

There is no registration or notice obligation to the Slovak Office as supervisory authority required anymore.

# Data protection officers

## EU regulation

Each controller or processor is required to appoint a data protection officer if it satisfies one or more of the following tests:

- it is a public authority;
- its core activities consist of processing operations which, by virtue of their nature, scope or purposes, require regular and systemic monitoring of data subjects on a large scale; or
- its core activities consist of processing sensitive personal data on a large scale.

Groups of undertakings are permitted to appoint a single data protection officer with responsibility for multiple legal entities (Article 37(2)), provided that the data protection officer is easily accessible from each establishment (meaning that larger corporate groups may find it difficult in practice to operate with a single data protection officer).

DPOs must have "*expert knowledge*" (Article 37(5)) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6)).

Controllers and processors are required to ensure that the DPO is involved "*properly and in a timely manner in all issues which relate to the protection of personal data*" (Article 38(1)), and the DPO must directly report to the highest management level, must not be told what to do in the exercise of his or her tasks and must not be dismissed or penalised for performing those tasks (Article 38(3)).

The specific tasks of the DPO, set out in GDPR, include (Article 39):

- to inform and advise on compliance with GDPR and other Union and Member State data protection laws;
- to monitor compliance with the law and with the internal policies of the organization including assigning responsibilities, awareness raising and training staff;
- to advise and monitor data protection impact assessments where requested; and
- to cooperate and act as point of contact with the supervisory authority.

This is a good example of an area of the GDPR where Member State gold plating laws are likely. For example, German domestic law has set the bar for the appointment of DPOs considerably lower than that set out in the GDPR.

## Slovak Republic regulation

There is an online form on the website of the Slovak Office which should be completed in order to notify the supervisory authority of the appointment of a DPO.

# Collection and processing

## EU regulation

### Data Protection Principles

Controllers are responsible for compliance with a set of core principles which apply to all processing of personal data. Under these principles, personal data must be:

- Processed lawfully, fairly and in a transparent manner (the "lawfulness, fairness and transparency principle")
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (the "purpose limitation principle")
- Adequate, relevant and limited to what is necessary in relation to the purpose(s) (the "data minimization principle");
- Accurate and where necessary kept up to date (the "accuracy principle")
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose(s) for which the data are processed (the "storage limitation principle")
- Processed in a manner that ensures appropriate security of the personal data, using appropriate technical and organizational measures (the "integrity and confidentiality principle")

The controller is responsible for and must be able to demonstrate compliance with the above principles (the "accountability principle"). Accountability is a core theme of the GDPR. Organizations must not only comply with the GDPR but also be able to *demonstrate* compliance for potentially years after a particular decision relating to processing personal data was rendered. Record-keeping, auditing and appropriate governance will all play a key role in achieving accountability.

### Legal Basis under Article 6

In addition, in order to satisfy the lawfulness principle, each use of personal data must be justified by reference to an appropriate basis for processing. The legal bases (also known lawful bases or lawful grounds) under which personal data may be processed are (Article 6(1)):

- With the consent of the data subject (where consent must be "*freely given, specific, informed and unambiguous*", and must be capable of being withdrawn at any time)
- Where necessary for the performance of a contract to which the data subject is party, or to take steps at the request of the data subject prior to entering into a contract
- Where necessary to comply with a legal obligation (of the EU) to which the controller is subject
- Where necessary to protect the vital interests of the data subject or another person (generally recognised as being limited to 'life or death' scenarios, such as medical emergencies)
- Where necessary for the performance of a task carried out in the public interest, or in the exercise of official authority vested in the controller
- Where necessary for the purposes of the legitimate interests of the controller or a third party (which is subject to a balancing test, in which the interests of the controller must not override the interests or fundamental rights and freedoms of the data subject. Note also that this basis cannot be relied upon by a public authority in the performance of its tasks)

### Special Category Data

Processing of special category data is prohibited (Article 9), except where one of the following exemptions applies (which, in effect, operate as secondary bases which must be established for the lawful processing of special category data, in addition to an Article 6 basis):

- With the explicit consent of the data subject
- Where necessary for the purposes of carrying out obligations and exercising rights under employment, social security and social protection law or a collective agreement
- Where necessary to protect the vital interests of the data subject or another natural person who is physically or legally incapable of giving consent
- In limited circumstances by certain not-for-profit bodies
- Where processing relates to the personal data which are manifestly made public by the data subject
- Where processing is necessary for the establishment, exercise or defence of legal claims or where courts are acting in their legal capacity
- Where necessary for reasons of substantial public interest on the basis of Union or Member State law, proportionate to the aim pursued and with appropriate safeguards
- Where necessary for preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, provision of health or social care or treatment of the management of health or social care systems and services
- Where necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of health care and of medical products and devices

- Where necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with restrictions set out in Article 89(1)

Member States are permitted to introduce domestic laws including further conditions and limitations for processing with regard to processing genetic data, biometric data and health data.

### Criminal Convictions and Offences data

Processing of personal data relating to criminal convictions and offences is prohibited unless carried out under the control of an official public authority, or specifically authorized by Member State domestic law. (Article 10).

### Processing for a Secondary Purpose

Increasingly, organisations wish to re-purpose personal data - ie, use data collected for one purpose for a new purpose which was not disclosed to the data subject at the time the data were first collected. This is potentially in conflict with the core principle of purpose limitation; to ensure that the rights of data subjects are protected. The GDPR sets out a series of factors that the controller must consider to ascertain whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4)). These include:

- Any link between the original purpose and the new purpose
- The context in which the data have been collected
- The nature of the personal data, in particular whether special categories of data or data relating to criminal convictions are processed (with the inference being that if they are it will be much harder to form the view that a new purpose is compatible)
- The possible consequences of the new processing for the data subjects
- The existence of appropriate safeguards, which may include encryption or pseudonymisation

If the controller concludes that the new purpose is incompatible with the original purpose, then the only bases to justify the new purpose are consent or a legal obligation (more specifically an EU or Member State law which constitutes a necessary and proportionate measure in a democratic society).

### Transparency (Privacy Notices)

The GDPR places considerable emphasis on transparency, i.e. the right for a data subject to understand how and why his or her data are used, and what other rights are available to data subjects to control processing. The presentation of granular, yet easily accessible, privacy notices should, therefore, be seen as a cornerstone of GDPR compliance.

Various information must be provided by controllers to data subjects in a concise, transparent and easily accessible form, using clear and plain language (Article 12(1)).

The following information must be provided (Article 13) at the time the data are obtained:

- The identity and contact details of the controller
- The data protection officer's contact details (if there is one)
- Both the purpose for which data will be processed and the legal basis for processing, including, if relevant, the legitimate interests for processing
- The recipients or categories of recipients of the personal data
- Details of international transfers
- The period for which personal data will be stored or, if that is not possible, the criteria used to determine this
- The existence of rights of the data subject including the right to access, rectify, require erasure, restrict processing, object to processing and data portability
- Where applicable, the right to withdraw consent, and the right to complain to supervisory authorities
- The consequences of failing to provide data necessary to enter into a contract
- The existence of any automated decision making and profiling and the consequences for the data subject
- In addition, where a controller wishes to process existing data for a new purpose, they must inform data subjects of that further processing, providing the above information

Somewhat different requirements apply (Article 14) where information has not been obtained from the data subject.

## Rights of the Data Subject

Data subjects enjoy a range of rights to control the processing of their personal data, some of which are very broadly applicable, whilst others only apply in quite limited circumstances. Controllers must provide information on action taken in response to requests within one calendar month as a default, with a limited right for the controller to extend this period thereby a further two months where the request is onerous.

#### Right of access (Article 15)

A data subject is entitled to request access to and obtain a copy of his or her personal data, together with prescribed information about the how the data have been used by the controller.

#### Right to rectify (Article 16)

Data subjects may require inaccurate or incomplete personal data to be corrected or completed without undue delay.

#### Right to erasure ('right to be forgotten') (Article 17)

Data subjects may request erasure of their personal data. The forerunner of this right made headlines in 2014 when Europe's highest court ruled against Google (Judgment of the CJEU in Case C-131/12), in effect requiring Google to remove search results relating to historic proceedings against a Spanish national for an unpaid debt on the basis that Google as a data controller of the search results had no legal basis to process that information.

The right is not absolute; it only arises in quite a narrow set of circumstances, notably where the controller no longer needs the data for the purposes for which they were collected or otherwise lawfully processed, or as a corollary of the successful exercise of the objection right, or of the withdrawal of consent.

The Court of Justice of the European Union delivered two judgments on 24 September 2019 in case of 'Right to be forgotten'.

The first decision of the CJEU provides important explanations on the conditions under which persons may delete a link found in a search result if the linked page contains information related to sensitive information (such as their religion, their political opinion or the existence of a conviction for crime). It also provides useful information about the public's interest in accessing information that has become incomplete or outdated due to the passage of time (Judgment of the CJEU in Case C-136/17).

In its second decision, the CJEU decided on the geographical scope of the right to remove links from search results after entering the first name and last name. The CJEU limits the effect of the right of removal from search results to results from European territory only - in other words, removing results in the EU but not worldwide. Search results will therefore remain accessible based on searches conducted outside the European Union. (Judgment of the CJEU in Case C-507/17).

#### Right to restriction of processing (Article 18)

Data subjects enjoy a right to restrict processing of their personal data in defined circumstances. These include where the accuracy of the data is contested; where the processing is unlawful; where the data are no longer needed save for legal claims of the data subject, or where the legitimate grounds for processing by the controller are contested.

#### Right to data portability (Article 20)

Where the processing of personal data is justified either on the basis that the data subject has given his or her consent to processing or where processing is necessary for the performance of a contract, then the data subject has the right to receive or have transmitted to another controller all personal data concerning him or her in a structured, commonly used and machine-readable format (eg, commonly used file formats recognised by mainstream software applications, such as .xsl).

#### Right to object (Article 21)

Data subjects have the right to object to processing on the legal basis of the legitimate interests of the data controller or where processing is in the public interest.

Controllers will then have to suspend processing of the data until such time as they demonstrate “compelling legitimate grounds” for processing which override the rights of the data subject.

In addition, data subjects enjoy an unconditional right to object to the processing of personal data for direct marketing purposes at any time.

**The right not to be subject to automated decision making, including profiling (Article 22)**

Automated decision making (including profiling) "*which produces legal effects concerning [the data subject] … or similarly significantly affects him or her*" is only permitted where:

1. Necessary for entering into or performing a contract
2. Authorised by EU or Member State law
3. The data subject has given their explicit (ie, opt-in) consent

Further, where significant automated decisions are taken on the basis of grounds (a) or (c), the data subject has the right to obtain human intervention, to contest the decision, and to express his or her point of view.

---

## Slovak Republic regulation

Collection and processing of personal data is governed by the GDPR.

However, there is specific regulation in this respect in the fourth part of the Slovak Data Protection Act. Pursuant to Section 78 of the Slovak Data Protection Act, these specific situations are as follows:

- A controller may process personal data without the consent of a data subject if the processing of personal data is necessary for academic, artistic or for literary purposes;
- A controller may process personal data without the consent of a data subject if the processing of personal data is necessary for the purposes of informing the public by means of mass media and if the personal data are processed by a controller which is authorised to do such business activity;
- A controller who is the employer of a data subject is authorized to provide his / her personal data or to make public his / her personal data in the scope of academic title, name, surname, position, personal employee´s number, department, place of work performance, telephone number, fax number, work email address and the identification details of employer, if this is necessary in connection with the performance of the employment duties of a data subject. Such provision of personal data or making them public shall not interfere with the reputability, dignity and security of a data subject;
- In the processing of personal data, a birth number may be used for the purpose of identifying a natural person only if its use is necessary for the purpose of processing. A data subject shall grant the explicit consent. Processing of a birth

number on the legal basis of consent of a data subject shall not be excluded by a special regulation. Making public a birth number is prohibited; this does not apply if a data subject makes public a birth number;

- A controller may process genetic, biometric and health-related data on the legal basis of a special regulation or an international treaty to which the Slovak Republic is bound;
- Personal data on the data subject may be obtained from another natural person and processed in the information system with the prior written consent of data subject only; this does not apply if another natural person by providing personal data about the data subject to the information system, protects his own rights or legally protected interests, reports the facts that justify the application of legal liability of the data subject or personal data are processed on the basis of a special act. Upon request of Office, the person who processes such personal data must be able to prove to the Office that he / she has obtained personal data in accordance with this act.
- If a data subject is dead, the consent required may be given by a close person. The consent is not valid if at least one close person has disagreed in writing.
- If a data subject is dead, the consent required may be given by a close person. The consent is not valid if at least one close person has disagreed in writing.
- When processing personal data for archiving, scientific purposes, historical research or statistical purposes, the controller and the intermediary are obliged to accept adequate guarantees for the rights of the data subject. These guarantees shall include the establishment of adequate and effective technical and organizational measures, in particular to ensure compliance with the principles of data minimization and pseudonymisation. This does not apply to the processing of personal data of deceased persons.

## Transfer

### EU regulation

Transfers of personal data by a controller or a processor to third countries outside of the EU (and Norway, Liechtenstein and Iceland) are only permitted where the conditions laid down in the GDPR are met (Article 44).

The European Commission has the power to make an adequacy decision in respect of a third country, determining that it provides for an adequate level of data protection, and therefore personal data may be freely transferred to that country (Article 45(1)).

The European Commission has so far recognised Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Republic of Korea, Switzerland, the United Kingdom under the GDPR and the LED, the United States (commercial organisations participating in the EU-US Data Privacy Framework) and Uruguay as providing adequate protection.

With the exception of the United Kingdom, these adequacy decisions do not cover data exchanges in the law enforcement sector which are governed by the Law Enforcement Directive (Article 36 of Directive (EU) 2016/680).

The Commission is required to periodically review the adequacy decisions adopted under the GDPR and its predecessor, Directive 95/46/EC, and to report its findings to the European Parliament and the Council. In line with this obligation, the Commission published its Report on the first periodic review of the adequacy decision for Japan on 4 April 2023. On 15 January 2024 the Commission published its Report on the first review of the functioning of the eleven adequacy decisions adopted pursuant to Directive 95/46/EC. On 9 October 2024, the Commission published its Report on the first review of the functioning of the adequacy decision on the EU-US Data Privacy Framework.

Transfers to third countries are also permitted where appropriate safeguards have been provided by the controller or processor and on condition that enforceable data subject rights and effective legal remedies for the data subject are available. The list of appropriate safeguards includes amongst others binding corporate rules and standard contractual clauses. The GDPR has removed the need which existed in some Member States under the previous law to notify and in some cases seek prior approval of standard contractual clauses from supervisory authorities.

The GDPR (Article 49) also includes a list of context specific derogations, permitting transfers to third countries where:

a. explicit informed consent has been obtained;
b. the transfer is necessary for the performance of a contract or the implementation of pre-contractual measures;
c. the transfer is necessary for the conclusion or performance of a contract concluded in the interests of the data subject between the controller and another natural or legal person;
d. the transfer is necessary for important reasons of public interest;
e. the transfer is necessary for the establishment, exercise or defence of legal claims;
f. the transfer is necessary in order to protect the vital interests of the data subject where consent cannot be obtained; or
g. the transfer is made from a register which according to EU or Member State law is intended to provide information to the public, subject to certain conditions.

There is also a very limited derogation to transfer where no other mechanism is available and the transfer is necessary for the purposes of compelling legitimate interests of the controller which are not overridden by the interests and rights of the data subject; notification to the supervisory authority and the data subject is required if relying on this derogation.

Transfers demanded by courts, tribunals or administrative authorities of countries outside the EU (Article 48) are only recognised or enforceable (within the EU) where they are based on an international agreement such as a mutual legal assistance treaty in force between the requesting third country and the EU or Member State; a transfer in response to such requests where there is no other legal basis for transfer will infringe the GDPR.

## Slovak Republic regulation

Pursuant to the GDPR, the free movement of personal data between the Slovak Republic and EU Member States is guaranteed; the Slovak Republic shall not restrict or prohibit the transfer of personal data in order to protect the fundamental rights of natural persons, in particular their right to privacy in connection with the processing of their personal data.

The transfer of personal data to third countries or international organisations is governed by the GDPR.

## Security

### EU regulation

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 states that controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk of the processing. In so doing, they must take account of the state of the art, the costs of implementation, and the nature, scope, context and purposes of processing. A 'one size fits all' approach is therefore the antithesis of this requirement.

However the GDPR does require controllers and processors to consider the following when assessing what might constitute adequate security:

a. the pseudonymisation and encryption of personal data;
b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and
d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The rights and obligations in regard to the security of personal data are governed by the GDPR.

In this respect, the Slovak Office issued Decree No. 158/2018 Coll. on Procedure when Assessing the Impact on the Protection of Personal Data as of 29 May 2018.

### Slovak Republic regulation

Controllers and processors shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The rights and obligations in regard to the security of personal data are governed by the GDPR.

In this respect, the Slovak Office issued Decree No. 158/2018 Coll. on Procedure when Assessing the Impact on the Protection of Personal Data as of 29 May 2018.

## Breach notification

### EU regulation

The GDPR contains a general requirement for a personal data breach to be notified by the controller to its supervisory authority, and for more serious breaches to also be notified to affected data subjects. A personal data breach is a wide concept, defined as any "*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*." (Article 4).

The controller must notify a breach to the supervisory authority without undue delay, and where feasible, not later than 72 hours after having become aware of it, unless the controller determines that the breach is unlikely to result in a risk to the rights and freedoms of natural persons. When the personal data breach is likely to result in a high risk to natural persons, the controller is also required to notify the affected data subjects without undue delay. (Article 34).

Where the breach occurs at the level of the processor, it is required to notify the controller without undue delay upon becoming aware of the breach. (Article 33(2)).

The notification to the supervisory authority must include where possible:

- The categories and approximate numbers of individuals and records concerned
- The name of the organisation's data protection officer or other contact
- The likely consequences of the breach and the measures taken to mitigate harm
- The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Controllers are also required to keep a record of all data breaches (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

### Slovak Republic regulation

Breach notifications are governed by the GDPR.

## Enforcement

### EU regulation

#### Fines

The GDPR empowers supervisory authorities to impose fines of up to 4% of annual worldwide turnover, or EUR 20 million (whichever is higher).

It is the intention of the European Commission that fines should, where appropriate, be imposed by reference to the revenue of an economic undertaking rather than the revenues of the relevant controller or processor. Recital 150 of the GDPR states that 'undertaking' should be understood in accordance with Articles 101 and 102 of the

Treaty on the Functioning of the European Union, which prohibit anti-competitive agreements between undertakings and abuse of a dominant position. Unhelpfully, the Treaty does not define 'undertaking' and the extensive case-law is not entirely straightforward, with decisions often turning on the specific facts of each case. However, in many competition cases, group companies have been regarded as part of the same undertaking. The assessment will turn on the facts of each case, and the first test cases under the GDPR will need to be scrutinised carefully to understand the interpretation of 'undertaking'. Under EU competition law case-law, there is also precedent for regulators to impose joint and several liability on parent companies for fines imposed on those subsidiaries in some circumstances (broadly where there is participation or control), so-called "look through" liability. Again, it remains to be seen whether there will be a direct read-across of this principle into GDPR enforcement.

Fines are split into two broad categories.

The highest fines (Article 83(5)) of up to EUR 20 million or, in the case of an undertaking, up to 4% of total worldwide turnover of the preceding year, whichever is higher, apply to infringement of:

- the basic principles for processing including conditions for consent;
- data subjects' rights;
- international transfer restrictions;
- any obligations imposed by Member State law for special cases such as processing employee data; and
- certain orders of a supervisory authority.

The lower category of fines (Article 83(4)) of up to EUR 10 million or, in the case of an undertaking, up to 2% of total worldwide turnover of the preceding year, whichever is the higher, apply to infringement of:

- obligations of controllers and processors, including security and data breach notification obligations;
- obligations of certification bodies; and
- obligations of a monitoring body.

Supervisory authorities are not required to impose fines but must ensure in each case that the sanctions imposed are effective, proportionate and dissuasive (Article 83(1)).

Fines can be imposed in combination with other sanctions.

### Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58) including the power to undertake on-site data protection audits and the power to issue public warnings, reprimands and orders to carry out specific remediation activities.

### Right to claim compensation

The GDPR makes specific provision for individuals to bring private claims against controllers and processors:

- any person who has suffered "material or non-material damage" as a result of a breach of the GDPR has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress even where they are not able to prove financial loss.
- data subjects have the right to mandate a consumer protection body to exercise rights and bring claims on their behalf (Article 80).

Individuals also enjoy the right to lodge a complaint with a supervisory authority (Article 77).

All natural and legal persons, including individuals, controllers and processors, have the right to an effective judicial remedy against a decision of a supervisory authority concerning them or for failing to make a decision (Article 78).

Data subjects enjoy the right to an effective legal remedy against a controller or processor (Article 79).

## Slovak Republic regulation

The Slovak Office has various powers to ensure compliance with the Slovak Data Protection Act and the GDPR.

For example, the Slovak Office is entitled to:

- on request, provide information to a data subject in relation to the exercise of her / his rights;
- order a controller or a processor to provide the necessary information;
- order a data controller to notify a data subject of a personal data breach;
- enter the premises of a controller or a processor;
- impose a corrective measure or a fine.

# Electronic marketing

With effect as of 1 February 2022, the electronic marketing is regulated by the Act No. 452/2021 Coll. on Electronic Communications, as amended (the "**Act**"). With the effectiveness of the Act, the former regulation, i.e. Act No. 351/2011 Coll. on Electronic Communications, as amended, has been repealed.

The Act transposed Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing a European Electronic Communications Code into the Slovak law.

The Act introduced new requirements for obtaining consent and conditions for conducting direct marketing including its definition.

According to the Act, the direct marketing means any form of presentation of goods or services in written or oral form, sent or presented through a publicly available service directly to one or more subscribers or users.

The Act stipulates that the use of automatic call and communication systems without human intervention, fax, e-mail and SMS and MMS message service is permitted towards the subscriber or user only with his / her prior demonstrable consent obtained before contacting the subscriber or user. For the purposes of obtaining prior consent, the use of automatic calling and communication systems without human intervention, fax, electronic mail and short message service is prohibited.

Consent that meets the requirements of Article 4 (11) GDPR is considered to be demonstrable consent for the purposes of direct marketing. The person to whom such consent was granted is obliged to keep a durable medium on which the demonstrable consent of the subscriber or user is recorded for a period of at least four years from the withdrawal of the consent by the subscriber or user. When obtaining the consent of the subscriber or user, the person carrying out direct marketing is obliged to indicate the way in which the consent can be easily revoked.

The subscriber or user can at any time withdraw the previous consent or object to the call for the purpose of direct marketing or obtaining consent. The person to whom such consent has been revoked or to whom the call has been objected is obliged to demonstrably confirm to the subscriber or user the revocation of such consent or the acceptance of the objection to the call no later than 30 days after the date of revocation of consent or the receipt of the objection to the call and to keep the confirmation of the revocation of the consent or the acceptance of the objection to the call on a durable medium for a period of at least four years from the withdrawal of consent or call objections.

The Act introduced also the list of the phone numbers, which will be held by the Office for Electronic Communications and Postal Services and which will include the phone numbers stipulated by subscribers or users for the purpose of expressing disagreement with the call for direct marketing purposes and for verifying the listing of a telephone number or group of telephone numbers by the person carrying out direct marketing in the list of telephone numbers (the "**list**").

For the purposes of direct marketing, any call is prohibited if the subscriber or user has:

- provided a phone number in the list; or
- objected to such calls to the person for whose benefit direct marketing is carried out (this does not apply if the subscriber or user revoked the objection to calls for the purposes of direct marketing to the person for whose benefit direct marketing is carried out or granted his / her consent in the time after the last update of the phone number in the list).

The prior consent of the recipient of electronic mail, SMS and MMS message service is not required if it is a direct marketing of a person's own similar goods and services, and if his / her contact details for the delivery of electronic mail, SMS and MMS message service were obtained by the same person in connection with the sale of

goods or services, or if it is direct marketing addressed to the published contact details of subscriber or user who is a natural person - entrepreneur or legal entity. The recipient of electronic mail, SMS and MMS message service must be given the opportunity to simply and free of charge at any time to refuse such use of the contact data at the time of their acquisition and with each delivered message if he / she has not previously refused such use. It is forbidden:

i. to send electronic mail from which the identity and address of the sender is unknown, to which the recipient can send a request to stop sending such messages; and
ii. to encourage visitors to visit a website in violation with a special regulation.

## Online privacy

### EU regulation

As regards the protection of privacy and protection of personal data processed in the electronic communications sector, the provisions of the Act (Act No. 452/2021 Coll. On Electronic Communications, as amended) shall apply. The Act implemented e.g. Directive 2002/58/EC (as amended by Directive 2009/136/EC).

Under the Act, the undertaking company that provides a publicly available network or service or a provider of a publicly available service is obliged to ensure the technical and organizational confidentiality of messages and associated Traffic Data that are transmitted through its public network and publicly available services. In particular, it is prohibited to record, intercept, store messages or other types of interception or monitoring of messages and their associated data by persons other than the users or without the consent of the users concerned, unless regulated otherwise. This does not prevent the technical storage of data that are necessary for the transmission of messages, without prejudice to the principle of confidentiality.

Further to this, the undertaking company shall not be liable for the protection of transmitted messages if there is a possibility of their direct listening or unprotected acquisition at the place of transmission or at the place of reception.

However, this ban does not apply to temporary recording and storing of messages, as well as related Traffic Data if it is required:

- for the provision of value added services ordered by a subscriber or user;
- to prove a request to establish, change or withdraw the service; or
- to prove the existence or validity of other legal acts, which the subscriber, user or undertaking company has made.

Article 5 (3) of Directive No. 2002/58/EC of the European parliament and of the Council on concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) was implemented into Section 109 of the Act. Under Section 109 (8) of the Act: "*every person that stores or gains access to information stored in the terminal equipment of a user shall be authorised for that only if the user concerned has given his / her demonstrable consent. The obligation to obtain consent does not apply to law*

*enforcement authorities and other state authorities. This shall not prevent any technical storage of data or access hereof for the sole purpose of the conveyance or facilitation of the conveyance of a communication by means of a network or if strictly necessary for the provider of an information society service to provide information society services if explicitly requested by the user*."

Processing of cookies requires a demonstrable consent of the user. According to the opinion of the Office of Electronic Communication and Postal Services as the demonstrable consent according to the Act is considered such consent which met the conditions stipulated in Section 5 lit. a) of the Slovak Data Protection Act. In order for the consent to be freely given, access to services and features must not be conditional by the user's consent to the processing or storage of information through cookies. Access to the content, services or features on the website cannot be bound or conditioned by the granting such consent. Conditional use of the website by providing the user's consent with processing or storing information through cookies is a violation of Section 109 (8) of the Act.

## Slovak Republic regulation

### Traffic Data

Traffic Data are data related to the user and to the specific transmission of information in the network and arising during this transmission, which are processed for the purposes of transmission of messages in the network or for invoicing purposes. The Traffic Data related to subscribers or users may not be stored and the undertaking company is required, after the end of a communication transmission, without delay, to destroy or make anonymous such Traffic Data, except as provided otherwise by the Act.

If it is necessary for the invoicing of the subscribers and network interconnection payments, the undertaking company is required to store the Traffic Data until the expiration of the period during which the invoice may be legally challenged or the claim for the payment may be asserted. The undertaking company is required to provide the Traffic Data to the Office for Electronic Communications and Postal Services or the court in the case of a dispute between undertaking companies or between an undertaking company and a subscriber. In the event of a complaint, alternative dispute resolution, out-of-court dispute resolution or legal proceedings, in particular disputes relating to network connection or invoicing, the undertaking company must retain Traffic Data until the expiry of the period for all legal remedies. The scope of the stored Traffic Data must be limited to the minimum necessary.

The undertaking company is further authorized to process Traffic Data and Location Data (as described below) to the necessary extent even without the user's consent for the purposes:

- network operations, services or networks and services;
- accounting for the provided service, invoicing and proof of entitlement to payment for the provided service in debt collection;
- dealing with questions, complaints and claims of users;
- prevention and detection of security incidents and illegal actions; or

- providing cooperation to authorized state authorities.

The provider of a publicly available service may process the Traffic Data of the subscriber or user for the purposes of marketing services or for the purpose of providing value added services only with his / her prior consent and only to the extent and during the time necessary for marketing services and providing value added services. The undertaking company is obliged to inform the subscriber or user before obtaining his / her consent about the type of Traffic Data, the purpose of processing Traffic Data and the time of processing of this data. The subscriber or user may at any time revoke their consent to the processing of Traffic Data for marketing purposes or to provide value added services.

### Location Data

Location Data are data processed in the network or through the service that indicates the geographic location of the end device of the user of the publicly available service. The undertaking company may process the Location Data other than the Traffic Data which relates to the subscriber or the user of a public network or public service only if the data are made anonymous or the processing is done with consent of the user or subscriber of a public network or publicly available service, and in the scope and time necessary for the provision of the value added service or if the Act provides so. The undertaking company must, prior to obtaining consent, inform the subscriber or user of the Location Data other than Traffic Data which will be processed, on the type of Location Data to be processed, on the purpose and duration of the processing, and whether the data will be provided to a third party for the purpose of the provision of the value added service.

The subscriber or user may revoke its consent for the processing of Location Data at any time. If the subscriber or user has agreed to the processing of Location Data other than Traffic Data for the provision of a value added service, the undertaking company is obliged to allow him / her to temporarily refuse the processing of such Location Data in a simple way and free of charge every time he / she connects to the network or every time he / she transmits a message. The processing of Location Data, as described in previous sentences, shall be limited to persons acting on behalf of an undertaking company providing public networks or publicly available services, or to persons of a third party providing a value-added service and must be limited to the necessary purposes of providing a value added service.

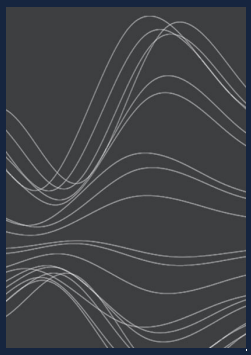
## Data protection lawyers

Michaela Stessl
Partner
DLA Piper
michaela.stessl@dlapiper.com
View bio

Eva Skottke
Legal Director
DLA Piper
eva.skottke@dlapiper.com
View bio

## For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



**Carolyn Bigg**
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

**John Magee**
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

**Andrew Serwin**
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

## About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com