DATA PROTECTION LAWS OF THE WORLD

Slovenia

DLA PIPER

SLOVENIA

Last modified 17 January 2024

LAW

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 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 the 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.

The new Slovenian Data Protection Act (ZVOP-2) which implements certain aspects of the GDPR has been adopted in December 2022 and has entered into force on 26 January 2023. From thereon, data protection is regulated by three main legal acts: (i) ZVOP-2; (ii) GDPR and (iii) Slovenian Act on the Protection of Personal Data in the Area of Treatment of Criminal Offences (*Zakon o varstvu osebnih podatkov na področju obravnavanja kaznivih dejanj*, Official Gazette no. 177/20; ZVOPOKD), which has entered into force on 31 December 2020 and implements Directive 2016/680. In relation to ZVOP-2, ZVOPOKD is considered lex specialis, therefore provisions of ZVOP-2 will not be used for questions specifically provided for and regulated by ZVOPOKD.

ZVOP-2 also regulates certain areas of data processing, not regulated by GDPR, namely:

- processing of personal data of deceased persons;
- processing of personal data in relation to carrying out activities outside of EU-law scope; and
- processing of personal data by the authorities of Slovenia when acting in areas of security and defence policy and carrying out intelligence and security activities.

Certain other Slovenian acts also regulate personal data processing, which is not set forth by GDPR, i.e.:

- Defence Act (*Zakon o obrambi*, Official Gazette no. 103/04 as amended from time to time and in force);
- Slovenian Intelligence and Security Agency Act (*Zakon o Slovenski obveščevalno-varnostni agenciji*; Official Gazette no. 81/06 as in force);
- Attorneys Act (*Zakon o odvetništvu*, Official Gazette no. 18/93 as amended from time to time and in force);
- Classified Information Act (*Zakon o tajnih podatkih*; Official Gazette no. 50/06 as amended from time to time and in force);
- Electronic Communications Act (*Zakon o elektronskih komunikacijah*, Official Gazette no. 130/22 as in force);
- Minor Offences Act (*Zakon o prekrških*; Official Gazette no. 29/11 as amended from time to time and in force);
- Patients’ Rights Act (*Zakon o pacientovih pravicah*; Official Gazette no. 15/08 as amended from time to time and in force);
- Mass Media Act (*Zakon o medijih*; Official Gazette no. 110/06 as amended from time to time and in force);
- Banking Act (*Zakon o bančništvu*; Official Gazette no. 92/21 and 123/21 as in force);
- Public Procurement Act (*Zakon o javnem naročanju*; Official Gazette no. 91/15 as amended from time to time and in

force);
- Employment Relationship Act (*Zakon o delovnih razmerjih*; Official Gazette no. 21/13 as amended from time to time and in force).

In accordance with Article 3(3) ZVOP-2, the above-listed acts are considered lex specialis in relation to ZVOP-2, meaning that provisions of ZVOP-2 will be applicable subsidiarily, when certain questions are not covered by the above-mentioned acts. Despite that, provisions of Articles 4-7 and 9-23 of GDPR would still apply *mutatis mutandis*, when such applicability is possible and appropriate (for instance in matters of threat to national security national legal provisions would prevail over the provisions of GDPR).

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 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.

In addition to the above, provisions of ZVOP-2 (together with GDPR) will apply when:

- processing of personal data is carried out within the public sector of Slovenia (Article 4(1) ZVOP-2); or
- processing of personal data is carried out within private sector when the following conditions are met:
    - the processor and / or controller is established in Slovenia, even if the processing of personal data does not take place in Slovenian territory (Article 4(1) ZVOP-2); or
    - the processor and / or controller is established outside EU but carries out activities of “offering services and goods” to persons domiciled in Slovenia in relation to person data processing, irrespective of whether a payment of data subject is required or are in relation to monitoring of data subjects’ behaviour (Article 4(2) ZVOP-2).

DEFINITIONS

In accordance with Article 5(1) ZVOP-2, terms used in ZVOP-2 have the same meaning as terms defined by Article 4 GDPR.

"**Personal data**" is defined as "*any information relating to an identified or identifiable natural person*" (Article 5(1) ZVOP-2 in connection with Article 4 GDPR). A low bar is set for "**identifiable**" – meaning a personal identification number; and any other (by law) defined unique identifiers of individuals by means of which it is possible to collect or retrieve personal data from personal data files in which unique identifier are processed; and other similar signs which are used regularly or systematically for linking databases between different controllers or between two or several files within one controller; a name is not necessary – any identifier will do, such as an identification number, phone number, location data or other factors which may identify that natural person (Article 5(2-V.) ZVOP-2).

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

ZVOP-2 contains more restrictive rules for the processing of "**special categories**" of personal data (including data relating to race, religion and nationality (Article 6(5) ZVOP-2), genetics and biometrics (Articles 81-84 ZVOP-2)) and personal data relating **to criminal convictions and offences** (Article 10 ZVOP-2), which do not differentiate from provisions of Article 9-10 GDPR. Additionally, ZVOP-2 creates rules regulating personal data relating to deceased persons (Article 9 ZVOP-2). Such personal data may be processed by either data processors authorized by law, family members, any entities who have legal interest exercising their rights before Slovenian authorities or to whom the deceased had given their consent for such processing prior to their passing. Provisions of Article 9 ZVOP-2 apply for 20 years after individuals passing away, unless otherwise provided by law.

ZVOP-2 together with 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 5(1) ZVOP-2 in connection with Article 4 GDPR). The processor "processes personal data on behalf of the controller", acting on the instructions of the controller. In contrast to the previous law, the ZVOP-2 together with 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.

NATIONAL DATA PROTECTION AUTHORITY

Enforcement of the GDPR is the prerogative of data protection regulators, known as supervisory authorities (for example, 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 Regulation.

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" (Article 56(1)).

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 (Article 56(2)).

The concept of lead supervisory authority is therefore of somewhat limited help to multinationals.

The Slovenian Data Protection Authority *(Informacijski pooblaščenec)* can be contacted as follows:

Informacijski pooblaščenec
Dunajska cesta 22, 1000 Ljubljana
Slovenia / Europe

Phone number: +386 1 230 97 30

Enail: gp-ip@ip-rs.si

REGISTRATION

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 organization and must be provided to supervisory authorities on request. This is a sizeable operational undertaking.

DATA PROTECTION OFFICERS

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) GDPR), 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) GDPR) of data protection law and practices, though it is possible to outsource the DPO role to a service provider (Article 37(6) GDPR).

It should be noted that ZVOP-2 provides for two other requirements for appointment of DPOs, namely: (a) legal capacity and (b) that the person has not been sentenced to a minimum term of imprisonment of six months or has not been the subject of a final conviction for a criminal offence relating to the misuse of personal data. Additional conditions also vary depending on whether the DPO works in a public authority, public sector (other than public authority) or in the private sector.

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) GDPR), 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 penalized for performing those tasks (Article 38(3) GDPR).

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

- 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.

In accordance with Article 48 ZVOP-2, DPO performs tasks listed in Article 39 GDPR, and specifically, provides advice on risk assessments regarding the security of personal data related to all processing of personal data in databases which is carried out by the controller or processor to whom they are assigned.

COLLECTION & PROCESSING

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 (Article 5 GDPR):

- 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"); and
- 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 perhaps years after a particular decision relating to processing personal data was taken. Record keeping, audit and appropriate governance will all form 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) GDPR):

- 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 recognized 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; or
- 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 GDPR), 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 Article 6 GDPR 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 defense 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; or
- 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) GDPR.

ZVOP-2 includes further conditions and limitations for processing with regard to processing genetic data, biometric data and data related to ethnicity and race. Part 13 of Patients’ Rights Act sets forth further limitations with regard to processing 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 GDPR).

In accordance with Article 10(2) ZVOP-2, processing of personal data relating to criminal convictions and offences is only allowed if it so prescribed by the law, including:

- further specification of the purpose of such processing, which must be in the public interest;
- types of data which can be processed;
- data subjects;
- entities / individuals to whom such data can be disclosed;
- specification of purpose of disclosure including its limitations;
- data retention limits; and
- measures ensuring lawful and fair processing.

Processing for a Secondary Purpose

Increasingly, organizations wish to 're-purpose' personal data - i.e. 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 ascertaining whether the new process is compatible with the purposes for which the personal data were initially collected (Article 6(4) GDPR). 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; and
- the existence of appropriate safeguards, which may include encryption or pseudonymization.

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).

Additionally, in accordance with Article 7 ZVOP-2 processing of personal data for secondary purposes is only possible if the processing is:

- in public interest;
- done by authorities in the public sector, when carrying out their legal obligations;
- allowed based on the law; and
- done in accordance with Article 6(4) GDPR.

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) GDPR).

The following information must be provided (Article 13 GDPR) 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; and
- 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 GDPR) 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 GDPR)

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 GDPR)

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 GDPR)

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.

Right to restriction of processing (Article 18 GDPR)

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 GDPR)

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 (e.g. commonly used file formats recognized by mainstream software applications, such as .xsl).

Right to object (Article 21 GDPR)

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 GDPR)

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

a. necessary for entering into or performing a contract;
b. authorised by EU or Member State law; or
c. the data subject has given their explicit (i.e. 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.

ZVOP-2 adds only specifications to the general processing requirements. The age for consent of children for the purposes of Article 8(1) GDPR is 15 years, unless general terms and conditions of the processor set forth a higher age limit. If consent is given by children under age 15, it is only valid if it is approved by the child’s parent or legal guardian.

ZVOP-2 sets forth further requirements regarding special areas of personal data processing:

a. processing of personal data for the purposes of scientific research, statistical research and for historic / archival purposes;

   For such purposes, processing of personal data (including special categories of personal data) is allowed by organizations and / or researchers if in the course of their activities they apply ethical principles and methodology in accordance with their field of research.

   Processing is permitted if:
   a. it is permitted by law; or
   b. the data subject has not prohibited processing of his / her personal data for such research purposes; or
   c. the data subject has given written consent for the processing of his / her personal data if personal data means professional secrecy.

      Furthermore, research organizations and / or researchers can access certain types of personal data if they fulfil specific conditions and requirements.

b. processing of personal data in the context of exercising freedom of speech;

   Under certain circumstances, especially if personal data has already been publicly disclosed, if individuals cannot expect protection of his / her privacy or the public interest exists, personal data can be published and processed when exercising freedom of speech.

c. video surveillance;

   If authorized persons want to introduce video surveillance, they must publish a notification. Apart from requirements provided for in Article 13(1) GDPR, the controller must publish some additional information either on the site or on websites. If such notification is published, it can be subsumed that the individual has been informed about video surveillance. Videos can be stored in accordance with Article 5 GDPR for up to 1 year since the video has been made.

   In any case, video surveillance is prohibited in elevators, toilets, hotel rooms, changing rooms and any premises in which

the individual expects higher level of protection of his / her privacy.

Some further conditions and requirements are set forth for video surveillance in workplaces, business premises, public transport, or public places.

d. processing of biometric and genetic data;

Processing of biometric and genetic data is very restricted and is only allowed if certain conditions / circumstances in accordance with ZVOP-2 are met.

e. evidence of entrance and exists in business premises;

f. publicly available databases;

g. data processing of contact data and personal documents of employees and / or other individuals who are key contacts for conducting a business (both in the private and public sector).

TRANSFER

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 GDPR).

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) GDPR).

Currently, the following countries or territories enjoy adequacy decisions: Andorra, Argentina, Canada (with some exceptions), Switzerland, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, Japan, Republic of Korea, United Kingdom (under the GDPR and the Law Enforcement Directive), Eastern Republic of Uruguay and New Zealand.

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 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 GDPR) 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.

No general additional requirements relating to transfers are introduced by ZVOP-2.

For more information, please visit our Transfer - global data transfer methodology website.

SECURITY

The GDPR is not prescriptive about specific technical standards or measures. Rather, the GDPR adopts a proportionate, context-specific approach to security. Article 32 GDPR states that controllers and processors shall implement appropriate technical and organizational 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 pseudonymization 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 organizational measures for ensuring the security of the processing.

ZVOP-2 provides no general additional requirements in relation to security measures. In the context of archiving, scientific or historical research purposes or statistical purposes, the ZVOP-2 sets out specific rules including anonymization or pseudonymization requirements.

Security measures are also detailed for each special regime but resemble the GDPR.

However, Article 22 ZVOP-2 provides additional requirements regarding data security by prescribing the so‑called "processing log" (dnevnik obdelave), namely by specifying:

- who must ensure processing logs;
- for which processing activities;
- what the processing log must contain;
- for which purposes the processing log can be used; and
- data retention periods in processing logs.

Article 23 ZVOP-2 specifies data security requirements in the field of special processing. These requirements apply to particularly risky information systems processing large amounts of sensitive, confidential, or otherwise protected data, including special categories of personal data.

Article 21 ZVOP-2 also includes provisions related to the protection of personal data in proceedings related to such personal data.

BREACH NOTIFICATION

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, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed*" (Article 4 GDPR).

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 GDPR).

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) GDPR).

The notification to the supervisory authority must include where possible the categories and approximate numbers of individuals and records concerned, the name of the organization’s data protection officer or other contact, the likely consequences of the breach and the measures taken to mitigate harm (Article 33(3) GDPR).

Controllers are also required to keep a record of all data breaches (Article 33(5) GDPR) (whether or not notified to the supervisory authority) and permit audits of the record by the supervisory authority.

In relation to data breaches, in Article 23 ZVOP-2 regulates data security in the field of special processing, which also involves reporting breaches. This article specifies that for certain information systems, the provisions on security requirements and reporting incidents from the Information Security Act (*Zakon o informacijski varnosti*) apply mutatis mutandis. These provisions concern essential service providers if the controller is not obliged to implement measures under the Information Security Act for these processing activities. Localization rules apply exist in case of special processing of personal information within information systems in which processing of the following categories of personal data is carried out: personal data specified in the laws governing administrative internal affairs, financial administration, citizenship, the Slovenian Intelligence and Security Agency, defence, healthcare, mandatory health insurance, the exercise of rights deriving from public funds, and criminal and minor offence records. Such data records must be kept within the territory of the Republic of Slovenia.

ENFORCEMENT

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) GDPR) 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) GDPR) 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) GDPR).

Fines can be imposed in combination with other sanctions.

It should be noted that the Slovenian Information Commissioner (*Informacijski pooblaščenec*) can impose fines on the basis of ZVOP-2.

Investigative and corrective powers

Supervisory authorities also enjoy wide investigative and corrective powers (Article 58 GDPR) 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) GDPR) 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 GDPR).

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

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 GDPR).

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

No general additional requirements are inserted in ZVOP-2.

ELECTRONIC MARKETING

The GDPR will apply to most electronic marketing activities, as these will involve some use of personal data (e.g. an email address which includes the recipient's name). The most plausible legal bases for electronic marketing will be consent, or the legitimate interests of the controller (which is expressly referenced as an appropriate basis by Recital 47 GDPR). Where consent is relied upon, the strict standards for consent under the GDPR are to be noted, and marketing consent forms will invariably need to incorporate clearly worded opt-in mechanisms (such as the ticking of an unticked consent box, or the signing of a statement, and not merely the acceptance of terms and conditions, or consent implied from conduct, such as visiting a website).

Data subjects have an unconditional right to object to (and therefore prevent) any form of direct marketing (including electronic marketing) at any time (Article 21(3) GDPR).

Specific rules on electronic marketing (including circumstances in which consent must be obtained) are to be found in Directive 2002/58/EC (ePrivacy Directive), as transposed into the local laws of each Member State. The ePrivacy Directive is to be replaced by a Regulation. However, it is currently uncertain when this is going to happen, as the European Commission has discarded its

draft of the ePrivacy Regulation after disagreements by the Member States in the Council of the European Union. In the meantime, GDPR Article 94 makes it clear that references to the repealed Directive 95/46/EC will be replaced with references to the GDPR.

As such, references to the Directive 95/46/EC standard for consent in the ePrivacy Directive will be replaced with the GDPR standard for consent.

Direct marketing by means of electronic communications is regulated by the Consumer Protection Act (Zakon o varstvu potrošnikov, Official Gazette 130/22), the Electronic Commerce Market Act (*Zakon o elektronskem poslovanju na trgu*, Official Gazette 96/09 as amended from time to time and in force), the Electronic Communications Act (*Zakon o elektronskih komunikacijah* , Official Gazette no. 130/22) and ZVOP-2.

The consent of an individual is required for the purposes of electronic marketing. Direct marketing is allowed where the "similar service / product" exemption applies, however customers must be given clear and distinct opportunity to refuse the use of their electronic mail address at the time of the collection of these contact details, and on the occasion of every message in the event that the customer has not initially refused such use. Additionally, the sending of electronic mail for the purposes of direct marketing, which disguises or conceals the identity of the sender, or is sent without a valid address, is prohibited.

ONLINE PRIVACY

Traffic data

Traffic Data must be erased or made anonymous as soon as it is no longer needed for the purpose of the transmission of a communication, except in cases where a longer period of retention is statutory allowed. Nevertheless, an operator may, until complete payment for service is made but no later than by expiry of the limitation period, retain and process traffic data required for the purposes of calculation and of payment relating to interconnection.

Location data

Location Data may only be processed for the purposes of providing the value-added service and when it is made anonymous, or with the prior consent of the user or subscriber, who may withdraw this consent at any time. Prior to issuing consent, a user or subscriber must be informed on (i) the possibility of refusing consent, (ii) the type of data to be processed, (iii) the purpose and duration of processing, and (iv) the possibility of the transmission of location data to a third party for the purpose of providing the value-added service.

Cookie compliance

The Electronic Communications Act (ZEKom-2) provides rules on the usage of cookies and similar technology for data storage.

Pursuant to ZEKom-2 the retention of information or the gaining of access to information stored in a subscriber’s or user’s terminal equipment (cookies) is only permitted if the subscriber or user gave their informed consent after having been given clear and comprehensive information about the information manager and the purpose of the processing of this information. However, an exception is provided in case of carrying out the transmission of a communication over an electronic communications network, or if this is strictly necessary for provision of service of information society explicitly requested by the subscriber or user.

KEY CONTACTS

Dr. Jasna Zwitter-Tehovnik
Partner
T +43 1 531 78 1042
jasna.zwitter-tehovnik@dlapiper.com

Domen Brus
Senior Associate
T +43 1 531 781848
domen.brus@dlapiper.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.