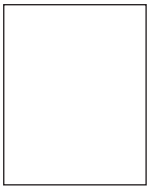
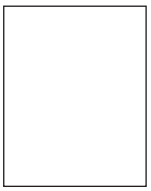
Chapter

# Slovenia

Luka Fabiani





CMS Reich-Rohrwig Hainz

Ela Omersa

## 1 Relevant Legislation and Competent Authorities

### 1.1 What is the principal data protection legislation?

The primary piece of legislation is the Personal Data Protection Act (*Zakon o varstvu osebnih podatkov, PDPA*) and its executive regulations. Moreover, the right to personal data protection is considered as a constitutional right and as such is defined in the Constitution of the Republic of Slovenia.

### 1.2 Is there any other general legislation that impacts data protection?

Several other acts govern data protection aspects such as the Electronic Communications Act (*Zakon o elektronskih komunikacijah; ECA*), Classified Information Act (*Zakon o tajnih podatkih*), Identity Card Act (*Zakon o osebni izkaznici*), Passports Act (*Zakon o potnih listinah*) and Protection of Documents and Archives and Archival Institutions Act (*Zakon o varstvu dokumentarnega in arhivskega gradiva ter arhivih*).

The duties and powers of the Information Commissioner are regulated in the Information Commissioner Act (*Zakon o informacijskem pooblaščencu*), whereas the Inspection Act (*Zakon o inšekcijskem nadzoru*), Minor Offences Act (*Zakon o prekrških*) and General Administrative Procedure Act (*Zakon o splošnem upravnem postopku*) lay down the ground principles and general rules of the inspection procedures, inspection measures and further judicial sanctions and remedies.

### 1.3 Is there any sector specific legislation that impacts data protection?

Data protection is also safeguarded in legislation in the field of the health system (Patient Rights Act; *Zakon o pacientovih pravicah*), banking and finance (Banking Act; *Zakon o bančništvu*), employment (Employment Relationship Act; *Zakon o delovnih razmerjih*), social security and social assistance systems, insurance, educational system, internet, telecommunications and post services, direct marketing and price games, media (Media Act; *Zakon o medijih*), as well as in civil, criminal and administrative procedures.

### 1.4 What is the relevant data protection regulatory authority(ies)?

In Slovenia, the supervision over the protection of personal data is entrusted to the Information Commissioner (Informacijski pooblaščenec, IC) - an autonomous and independent body which supervises both the protection of personal data as well as access to public information.

## 2 Definitions

### 2.1 Please provide the key definitions used in the relevant legislation:

- **"Personal Data"**

  Are any data relating to an individual, irrespective of the form in which they are expressed.

- **"Sensitive Personal Data"**

  Are data on racial, national or ethnic origin, political, religious or philosophical beliefs, trade-union membership, health status, sexual life and the entry in or removal from a criminal record or records of minor offences. Moreover, biometric characteristics could be classified as sensitive personal data if their use makes it possible to identify an individual in connection with any of the aforementioned circumstances.

- **"Processing"**

  Processing may be performed manually or by using automated technology (means of processing). The term "Processing of personal data" refers to any operation or set of operations performed in connection with personal data that are subject to automated processing or which in manual processing are part of a filing system. These operations are in particular: collection, acquisition, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, communication, dissemination or otherwise making available, alignment or connection, blocking, anonymising, erasure or destruction.

- **"Data Controller"**

  Is any natural or legal person or other public or private sector person, who alone or jointly with others determines the purposes and means of the processing of personal data as well as any person provided by the statute who also determines the purposes and means of processing.

- **"Data Processor"**

  Is a natural or a legal person that processes personal data on behalf and for the account of the data controller.

- **"Data Owner"**

  There is no specific definition.

- **"Data Subject"**

  Is defined as an "Individual", who is an identified or an

identifiable natural person to whom personal data relates. An identifiable natural person is one who can be directly or indirectly identified, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity, whereas the method of identification does not incur any significant costs or disproportionate effort as well as require a vast amount of time.

- **"Pseudonymous Data"**

  There is no specific national definition.

- **"Direct Personal Data"**

  There is no specific definition.

- **"Indirect Personal Data"**

  There is no specific definition.

- **Other key definitions**

- **"Client"** – Any natural or legal person, who concludes a contract with the provider of publicly available electronic communication services to provide such services.

- **"Automated processing"** - Processing of personal data using information technology means.

- **"Filing system"** - Is any structured set of data, containing at least one piece of personal data, which is accessible according to the criteria enabling the use or combination of the data, irrespective of whether the set is centralised, decentralised or dispersed on a functional or geographical basis. A structured set of data is a set of data organised in such a manner so as to identify or enable identification of an individual.

- **"Data recipient"** - Is a natural or legal person or other private or public sector person to whom personal data is supplied or disclosed.

- **"Supply of personal data"** - Is the supply or disclosure of personal data.

- **"Foreign recipient and foreign data controller"** - Is a recipient of personal data in a third country and/or a data controller in a third country.

- **"Third country"** - Is a country that is not a Member State of the European Union (EU) or a part of the European Economic Area (EEA).

- **"Filing system catalogue"**- Is a description of a filing system.

  **"Register of Filing Systems"** - Is a register containing data from filing system catalogues.

- **"Blocking"** - Is such labelling of personal data that restricts or prevents their further processing.

- **"Anonymising"** - Is such alteration to the form of personal data so that it can no longer be linked to the individual or where such link can only be made with disproportionate efforts or expenses as well as a disproportionate use of time.

## 3 Key Principles

### 3.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  Everyone has a constitutional right to access the collected data related to him/her. Specifically, the individual has the right to the following information: (i) data on the data controller and its representative; (ii) the purpose of processing of personal data; (iii) possible data recipient and/or processor; (iv) type of data and data collection and the consequences if data will not be provided voluntarily; and (v) information on the right to consult, transcribe, copy, supplement, correct, block or erase personal data.

- **Lawful basis for processing**

  Personal data shall be processed lawfully and fairly (principle of lawfulness and fairness). In particular, personal data may only be processed if the processing of personal data and the personal data being processed are provided by statute, or a person has given consent for the processing of certain personal data. The purpose of processing personal data must be provided by statute, and in cases of processing on the basis of a personal consent of the individual, the individual must be informed in advance in writing or in another appropriate manner of the purpose of processing. However, if processing of personal data is necessary to protect the life or body of an individual, his/her personal data may be processed irrespective of the fact that no statutory grounds for processing of such data exists.

- **Purpose limitation**

  Personal data may only be collected for specific and lawful purposes and may not be further processed in such a manner that their processing would be counter to these purposes, unless otherwise provided by statute.

- **Data minimisation**

  Is connected to the principle of proportionality (see below).

- **Proportionality**

  Personal data that are being processed must be adequate and to an extent appropriate in relation to the purposes for which they are collected and further processed. Thus the principle of proportionality sets two limitations on the processing of personal data. Firstly, data must be adequate, which means that only data that could actually serve the purpose of processing may be collected. Secondly, the data should also be appropriate with respect to the purpose of collection and further processing. Only data that are completely necessary for achieving the purpose could be collected; also the processing should not be excessive (principle of data minimisation).

- **Retention**

  Personal data processed for any purpose or purposes shall not be stored for longer than is necessary to achieve the purpose for which they were collected or further processed.

- **Other key principles**

- **Legality and legal protection**

  Article 38 of the Constitution states that the collection, processing, purpose of processing, supervision and protection of personal data is specified by law. Furthermore, it guarantees a right to judicial protection in the event of any abuse of such data.

- **Prohibition of discrimination**

  Protection of personal data shall be guaranteed to every individual irrespective of nationality, race, colour, religious belief, ethnicity, sex, language, political or other belief, sexual orientation, material standing, birth, education, social position, citizenship, place or type of residence or any other personal circumstance.

## 4 Individual Rights

### 4.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Access to data**

  The IC is obliged to permit anyone to consult the register of filing systems and to transcribe the data. The consultation and transcription of data must be free of charge and available on the same day, or no later than within 15 days, otherwise the request shall be deemed to have been refused.

Data controllers are also obliged to supply personal data to data recipients against payment of the supply cost.

- **Correction and deletion**

  On request of an individual to whom personal data relate, the data controller must supplement, correct, block or erase personal data which the individual proves as being incomplete, inaccurate or not up to date, or that they were collected or processed contrary to the statute. Such a request shall be lodged in writing or orally in an annotation with the data controller.

  The data controller shall be obliged to perform the supplementing, correction, blocking or deletion of personal data within 15 days of the request and to inform the person who lodged the request thereof, or to inform him/her of the reasons why it will not do so by the same deadline. The data controller must decide on an objection within the same deadline. If the data controller fails to do so, the request shall be deemed to have been refused.

- **Objection to processing**

  An individual has the right to object to the processing of his/her personal data. The data controller shall grant such objection if the individual demonstrates that the conditions for processing under the PDPA are not fulfilled.

  If the data controller does not grant such an objection, the individual has 7 days to request that the IC shall decide on whether the processing is in accordance with the provisions of the PDPA. The IC shall decide within two months of receipt of the request and the lodging of such request withholds the processing of personal data.

- **Objection to marketing**

  An individual may at any time request that the data controller permanently or temporarily ceases to use his/her personal data for the purpose of direct marketing. The data controller is obliged to fulfil such request within 15 days and within 5 subsequent days inform the individual who made the request. The costs of all actions of the data controller in relation to such request shall be borne by the data controller.

- **Complaint to relevant data protection authority(ies)**

  The IC is competent to undertake inspection supervision on the implementation of the provisions of the PDPA and to decide on an appeal of an individual when the data controller refuses his/her request for providing data, extract, list, examination, confirmation, information, explanation, transcript or copy in accordance with provisions of the PDPA.

  Individual who finds that his/her rights provided by the PDPA have been violated may request judicial protection for as long as such violation lasts.

- **Other key rights**

  Most of the individual's key rights have already been specified above, but for the purpose of completeness, following rights derive from the basic individual's right to information – the data controller shall be, based on the request of the individual, obliged:

- to enable consultation of the filing system catalogue;
- to certify whether data relating to him/her are being processed or not, and to enable him/her to consult personal data contained in a filing system that relates to him/her, and to transcribe or copy them;
- to supply him/her an extract of personal data contained in a filing system that relates to him/her;
- to provide a list of data recipients to whom personal data were supplied, when they were supplied, on what basis and for what purpose;
- to provide information on the sources on which records contained about the individual in a filing system are based, and on the method of processing;
- to provide information on the purpose of processing and the type of personal data being processed, and all necessary explanations in this connection; and
- to explain technical and logical-technical procedures of decision-making, if the controller is performing automated decision-making through the processing of personal data of an individual.

  If an individual believes his/her right to personal data protection has been breached, or that his/her data was not processed lawfully, he/she may request for the IC's opinion on the matter. If an individual believes his/her rights from the PDPA have been violated, he/she may request legal protection by filing a lawsuit at the Administrative Court of the Republic of Slovenia. In such case it is necessary to first request the respect of his/her legal rights from the data controller. If the individual has suffered any damage due to unlawful processing of his/her data, he/she may initiate action for compensation according to the general principles of the reimbursement of damages as regulated in the Obligations code (*Obligacijski zakonik*).

## 5 Registration Formalities and Prior Approval

### 5.1 In what circumstances is registration or notification required to the relevant data protection regulatory authority(ies)? (E.g., general notification requirement, notification required for specific processing activities.)

There is a general notification requirement of the data controller to the IC every time before carrying out any wholly or partly automatic processing operation or before adding a new category of information to the filing system. The notification must occur no later than 15 days prior to the start of data processing.

Most notable exemption exists for a data controller that employs 50 or less fulltime employees. Such exemption however, does not apply to the filing systems kept by data controllers in the public sector, notaries public, attorneys, detectives, bailiffs, private security providers, private healthcare workers, healthcare providers, and to data controllers that keep filing systems containing sensitive personal data and process sensitive personal data as a part of their registered activity.

### 5.2 On what basis are registrations/notifications made? (E.g., per legal entity, per processing purpose, per data category, per system or database.)

Notifications are made per filing system.

### 5.3 Who must register with/notify the relevant data protection authority(ies)? (E.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation.)

The PDPA does not define the legal form of the data controller that has to respect the obligation of notification; in general the PDPA applies to the processing of personal data if the data controller is established, has its seat or is registered in the Republic of Slovenia, or if a subsidiary of the data controller is registered in the Republic of Slovenia.

**5.4 What information must be included in the registration/notification? (E.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes.)**

In the notification, the data controller shall supply:

- the title of the filing system;
- data on the data controller (for natural person: personal name, address where activities are performed or address of permanent or temporary residence, and for sole trader his official name, registered office, seat and registration number; for legal person: title or registered office and address or seat of the data controller and registration number);
- the category of individuals to whom the personal data relate;
- the type of personal data in the filing system;
- purpose of processing;
- data recipients or categories of data recipients of personal data contained in the filing system;
- whether the personal data is transferred to a third country, to where, to whom and the legal grounds for such transfer;
- a general description of security of personal data;
- data on connected filing systems from official records and public books; and
- data on the representative if the data controller is from a third country (for natural person: personal name, address where activities are performed or address of permanent or temporary residence, and for sole trader his official name, registered office, seat and registration number; for legal person: title or registered office and address or seat of the data controller and registration number).

**5.5 What are the sanctions for failure to register/notify where required?**

A fine from EUR 4,170 to 12,510 may be imposed for a minor offence to the data controller for not ensuring that the filing system catalogue contains data provided by statute and/or failing to supply data for the needs of the register of filing systems.

**5.6 What is the fee per registration (if applicable)?**

No fee is applicable.

**5.7 How frequently must registrations/notifications be renewed (if applicable)?**

IC has to be notified of any changes with respect to the method, purpose or scope of the data processing within 8 days of the adoption of any such changes.

**5.8 For what types of processing activities is prior approval required from the data protection regulator?**

No approval or consent is required from the IC.

**5.9 Describe the procedure for obtaining prior approval, and the applicable timeframe.**

See above under question 5.7.

## 6 Appointment of a Data Protection Officer

**6.1 Is the appointment of a Data Protection Officer mandatory or optional?**

Optional. There is no obligation to appoint a data protection officer as such, but data controllers must specify the persons who are responsible for individual data collections/filing systems and specify the persons who, due to the nature of their work, are permitted to process certain types/kinds of personal data ("responsible person"). This obligation does not apply for data controllers with 50 or less full-time employees.

**6.2 What are the sanctions for failing to appoint a mandatory Data Protection Office where required?**

There are no sanctions prescribed.

**6.3 What are the advantages of voluntarily appointing a Data Protection Officer (if applicable)?**

See above under question 6.1.

**6.4 Please describe any specific qualifications for the Data Protection Officer required by law?**

No specific qualifications are prescribed.

**6.5 What are the responsibilities of the Data Protection Officer, as required by law or typical in practice?**

No specific responsibilities of a responsible person are prescribed; however, as such persons enforce the procedures and measures in relation to the security of personal data, it is expected that they practically implement all organisational, technical and logical-technical procedures and measures to protect personal data.

**6.6 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?**

No, this is not the case.

## 7 Marketing and Cookies

**7.1 Please describe any legislative restrictions on the sending of marketing communications by post, telephone, e-mail, or SMS text message (E.g., requirement to obtain prior opt-in consent or to provide a simple and free means of opt-out.)**

The data controller may use only certain personal data such as personal name, residence, telephone number, email address and fax number of individuals for further marketing activities if such data were collected in accordance with the law, meaning that the individual has explicitly consented to such use (prior opt-in consent). Individuals need to be informed about their right to demand at any time in writing or in another manner that the data controller shall permanently or temporarily cease to use their data for the purpose of direct marketing (right to recall).

Further, if personal data is going to be transferred to a third party for the purpose of direct marketing, a data controller should inform the individuals of this fact prior to the supply of their data and obtain a written consent. The individual shall also be notified about (i) which data is going to be transferred, (ii) who to, and (iii) for what purpose, whereas the costs of the notification shall be borne by the data controller.

Pursuant to the ECA, an explicit consent of an individual is needed prior to the use of an automated calling and communication system in order to contact an individual via telephone (automatic calling, SMS, MMS), fax or email. Differently, a company that obtained an email address from their clients may use it for direct marketing of similar products and/or service, under conditions that the customer is offered a clear and explicit possibility to reject such type of remittance by email.

### 7.2 Is the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

IC has issued several opinions interpreting rights and obligations about direct marketing, while it has issued only a few decisions based on its supervision powers, which were mostly only declaratory decisions stating a breach of the provisions of the PDPA.

### 7.3 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

A fine of EUR 2,080 to 4,170 shall be imposed on a legal person, sole proprietor or an individual independently performing an economic activity; whereas responsible persons may be fined from EUR 410 to 1,250 and individuals from EUR 200 to 830. Moreover, in relation to electronic communication the ECA prescribes even higher fines from EUR 1,000 to 20,000 for a middle or large sized company, EUR 200 to 1,000 for small companies, sole proprietors and individuals engaged in an economic activity and EUR 100 to 500 for their responsible persons.

### 7.4 What types of cookies require explicit opt-in consent, as mandated by law or binding guidance issued by the relevant data protection authority(ies)?

In principal, the ECA states that the use of cookies is only permitted if approved by the client or the user – opt-in option. In order to store data or gain access to information stored in the equipment of a client or a user, it is thus required to provide prior clear and comprehensive information on cookies' use, including information about the purposes of the processing as well as information on the data controller.

Notwithstanding the above general rule, cookies that are (i) necessary solely for the transmission of data over an electronic communication network, and (ii) absolutely necessary to insure the service of an IT company explicitly requested by the client or a user, do not require a prior opt-in consent. Based on the IC Guidelines on the usage of cookies on webpages, especially cookies that provide load balancing, user authentication, social media plug-in as well as flash cookies do not require a prior consent.

### 7.5 For what types of cookies is implied consent acceptable, under relevant national legislation or binding guidance issued by the relevant data protection authority(ies)?

The relevant legislation entails no explicit provision on the possibility of an implied consent. In that respect, the ECA only determines that the consent of an individual should mean a personal consent in accordance with PDPA. Moreover, the IC Guidelines indicate that implied consent (consent given by implied behaviour) may be possible; however, only in very restrictive cases (i.e. only in concrete cases where the consent could be unambiguously understood as an individual consent given in advance). Such implied consent mechanism should especially emphasize the notification on the usage of cookies which should be clearly visible (possible also on the subpages) also the individual should have the opportunity to subsequently change the settings of cookies. The reliability of this mechanism depends on: (i) the awareness of the users about cookies, (ii) the strength of invasion of cookies in the personal sphere of users, (iii) the limited "territorial" activity of the cookie, and (iv) its duration. In the opinion of the IC, usage of an implied consent is not appropriate in cases (i) where cookies allow tracking of users through different webpages, (ii) when processing sensitive personal data, and (iii) cookies with unlimited duration.

### 7.6 To date, has the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

Slovenia has successfully implemented the EU E-Privacy Directive (Directive 2002/58/EC) and Cookie Directive (Directive 136/2009/EC) in December 2012, whereas the deadline for the implementation of cookies provisions was 15 June 2013. For this reason the IC has only issued several opinions and so far no decision in an inspection procedure.

### 7.7 What are the maximum penalties for breaches of applicable cookie restrictions?

ECA prescribes the following fines: (i) up to EUR 20,000 for a legal person classified as a middle or large company; (ii) EUR 200 to 1,000 for a legal person classified as any other company, a sole proprietor or an individual engaged in an economic activity; and (iii) EUR 100 to 500 for a responsible person of such legal entity or a sole proprietor.

## 8 Restrictions on International Data Transfers

### 8.1 Please describe any restrictions on the transfer of personal data abroad?

The transfer of personal data to another Member State of the EU or the EEA is unimpeded. Nevertheless, when personal data is transferred to a third country, this may only be allowed under the condition that the IC issues a decision that the country, to which the data is transferred, ensures an adequate level of protection of personal data or if such a decision has already been taken. According to the IC, the following third countries ensure sufficient protection: Swiss Confederation, Republic of Macedonia and the USA. The latter provide an adequate level of protection of personal data insofar as personal data is transferred to organisations that operate under the internally established Safe Harbour principle.

### 8.2 Please describe the mechanisms companies typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions.

Most companies decide to transfer personal data abroad either (i) to their parent company or otherwise connecting companies, or (ii) to a cloud data provider. In case of transfer from a subsidiary to a

parent company, no special contract needs to be concluded since a subsidiary is not considered an independent legal person under the Slovenian law.

**8.3 Do transfers of personal data abroad require registration/notification or prior approval from the relevant data protection authority(ies)? Describe which mechanisms require approval or notification, what those steps involve, and how long they take.**

As in any other type of data transfer, the data controller needs to conclude a special written contract with the data processor, obtain a prior individual consent to such transmission and provide for concrete procedures and measures for security of personal data in their internal acts; moreover, a person responsible to process such data should be defined.

In case of transfer of personal data to the Member States of the EU and EEA as well as to third countries on the list of countries with an adequate level of protection, companies are free in the transmission and do not need any prior approval/notification. Nevertheless, if data is transferred to any other country, the company shall prior to the transfer obtain a positive decision from the IC on the adequate level of protection. For that purpose it shall file an application (accessible on the webpage of the IC), stating its legal interest in the issuing of a decision. The IC as well as the Ministry responsible for foreign affairs shall obtain additional information from the competent bodies in the third country as well as the EU. The final decision shall be issued two months after receipt of full information. The IC may also decide to issue a decision only for a certain type of data or for processing of data for an individual purpose.

## 9 Whistle-blower Hotlines

**9.1 What is the permitted scope of corporate whistle-blower hotlines under applicable law or binding guidance issued by the relevant data protection authority(ies)? (E.g., restrictions on the scope of issues that may be reported, the persons who may submit a report, the persons whom a report may concern.)**

In Slovenia, protection of whistle-blowers is ensured with Integrity and Prevention of Corruption Act (*Zakon o integriteti in preprečevanju korupcije*), which provides for legal protection of both civil servants and corporate employees. Any person may report instances of corruption in a State body, local community, by a holder of public authority or other legal persons governed by public or private law to a special Commission for the Prevention of Corruption or any other competent authority as well as inform the public of the corrupt practice in question. Classified data may, however, only be transmitted to criminal law enforcement authorities or to the Commission. Apart from that, civil servants are also encouraged to report any unethical or illegal conduct to their responsible person. Additional protection for civil servants is found in the Civil Servants Act (*Zakon o javnih uslužbencih*), which prohibits every humiliation, intimidation and insulting of one's dignity.

The data protection authority has so far issued no relevant guidance in this respect.

**9.2 Is anonymous reporting strictly prohibited, or strongly discouraged, under applicable law or binding guidance issued by the relevant data protection authority(ies)? If so, how do companies typically address this issue?**

Anonymous reporting is possible. The Integrity and Prevention of Corruption Act specifically states that the identity of the reporting person who submitted a report to the Commission in good faith and has reasonably believed that the information provided with regard to the report is true, shall not be established or disclosed. No additional rule exists in connection to the internal company whistle-blowing schemes.

**9.3 Do corporate whistle-blower hotlines require separate registration/notification or prior approval from the relevant data protection authority(ies)? Please explain the process, how long it typically takes, and any available exemptions.**

Based on the non-binding opinion of the IC, corporate whistle-blower hotlines in general do not need to be registered with the IC as a special filing system. Allegations that violations of law and regulations have occurred do not yet constitute facts about an individual, but merely represent a personal opinion of the whistle blower and thus do not represent personal data. On the other hand, when such allegations are thoroughly investigated, the facts that arise from such investigations may constitute personal data. Such personal data should be thus processed in accordance with provisions of PDPA, either as a part of an existing company's personnel files, which should be already registered with the IP, or as a separate filing system on investigated cases of whistle blowing, containing proven investigated facts about identified or identifiable individuals.

The notification of a filing system is obligatory only if the company of the data controller employs more than 50 employees (except for data controllers from the public sector, notary public, lawyers, detectives, executioners, private security companies, private health workers and health service providers and companies registered to process sensitive personal data, where the obligation is absolute) and should be done at least 15 days prior to the establishment of a new filing system or the entry of a new type of personal data. The process with the IC on average lasts only a week or two.

## 10 CCTV and Employee Monitoring

**10.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies)?**

The company conducting video surveillance must notify **individuals** of this fact, but needs no prior approval from the IC. Such notice must be visible and made public in a manner that enables individuals to acquaint themselves with the manner of surveillance, at the latest when the video surveillance of them begins. The notice shall contain information (i) that the video surveillance is taking place, (ii) the private or public entity executing the surveillance, (iii) a telephone number to obtain information as to where and for which period of time the recordings are being stored. Further notification formalities apply if **the CCTV** is used with respect to access to office and business premises, apartment buildings and work areas.

**10.2 What types of employee monitoring are permitted (if any), and in what circumstances?**

All types of employee monitoring are permitted only in exceptional cases, with due respect to the principle of proportionality and with respect to the right to privacy of the employees. Public and private entities may decide to implement video surveillance over the access to office and business premises, if necessary for the security of people or property, for ensuring supervision of entering and exiting or if a potential threat to employees exists. Moreover, video surveillance within work areas may be implemented in exceptional cases and as a last resort when necessarily required for the safety of people or property or to protect classified information and business secrecy. It should be limited to areas where the before mentioned interests need to be protected and is absolutely forbidden in work areas outside of the workplace, particularly in changing rooms, lifts and sanitary areas. Similar rules also apply to the use of biometrics.

In exceptional cases employers may decide to apply a GPS surveillance to their assets, e.g. vehicles. The use of GPS surveillance is only possible in rare cases when the right to property of the employers prevails over the right to privacy of the employees (e.g. extreme high value or importance of the content of the vehicles or other assets) or when reasons of personal safety of employees prevail over their right to privacy. Furthermore, employers are in no circumstances allowed to track company vehicles, when these are used for private purposes. Under exceptional circumstances the employer may also record telephone conversations of an employee as well as store such recordings, and monitor other electronic media (e.g. email, fax).

**10.3 Is consent or notice required? Describe how employers typically obtain consent or provide notice.**

Personal data of employees may only be processed if collection of such data is explicitly prescribed either by the Employment Legislation Act or other law or if the collection is necessary for the execution of rights and obligations arising out of employment relationship. In any other case, personal data of employees may only be processed under exceptional circumstances and after a written consent of an employee. Employees should be informed in writing prior to the commencement of the CCTV (either at the entry or at the workplace). Similarly, the employees should be notified in advance about the details of the GPS surveillance, in particular when the surveillance will take place, in which cases, how the GPS works, how to switch it on and off and what data will be collected. Moreover, the usage of such technology shall be in detail prescribed in an internal act that shall be made available to all affected employees.

**10.4 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?**

Prior to the introduction of video surveillance at the work place in a public or private entity, the employer shall consult the representative trade union.

**10.5 Does employee monitoring require separate registration/notification or prior approval from the relevant data protection authority(ies)?**

No special registration/notification is required. However, if personal data gathered through the CCTV or other types of monitoring are collected in a form of a filing system, such filing system should be duly registered with the IC.

## 11 Processing Data in the Cloud

**11.1 Is it permitted to process personal data in the cloud? If so, what specific due diligence must be performed, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

Personal data may be processed in the cloud if general requirements of the PDPA on the processing of personal data are respected. The data controller should conclude an agreement with a data processor (cloud operator), which should include an agreement on the procedure and technical and organisational measures on the security of personal data. Upon an individual request, the data controller must provide the individual with a list of data processors/recipients, to whom the data were supplied; when such data were transmitted; on what basis; and for what purpose.

So far the IC has dealt with this topic in a couple of non-binding opinions; moreover, the IC has published Cloud Computing and Data Protection guidelines.

**11.2 What specific contractual obligations must be imposed on a processor providing cloud-based services, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

The cloud data processor may only process personal data in accordance with the purpose of data processing and should ensure the security of personal data. For this purpose a written contract should include a detailed list of how the security of personal data is provided; especially how the premises and the equipment are secured, what kind of programme software is used, how the cloud service provider prevents unauthorised usage, where the data are stored (provisions on tracking of data), how the revisions of the system of service provider are conducted, information in the event of disclosure of data, etc. Such contract should also include a list of countries where the data would be kept as a special permission of the IC is needed for the transfer of data to certain countries. Moreover, the data processor should at the end of the cooperation return all data to the data controller and destroy the copies. In its guidelines the IC also promotes the usage of the Model Contractual Clauses prepared by the EU Commission, which in its opinion provide sufficient contractual regulation. Despite the fact that the IC has not issued any binding decision in this respect, it has warned that in its opinion quite a significant number of cloud service providers in the market do not ensure all procedures and measurements for the security of personal data as prescribed by the PDPA. Due to the fact that the data controllers are the ones liable for a correct transfer of data and that in reality the cloud service providers are superior in their market power, the IC has proposed to the data controllers to use a control list of the minimum requirements that the data processors should secure.

## 12 Big Data and Analytics

**12.1 Is the utilisation of big data and analytics permitted? If so, what due diligence is required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

The PDPA does not regulate the utilisation of big data and analytics expressively; however, it does refer to the automated processing of data (processing of personal data using information technology means).

According to Article 15 PDPA the automated data processing, in which a decision may be taken regarding an individual that could have legal effect or substantive influence in relation to him/her, and which is based solely on automated data processing intended for the evaluation of certain personal aspects relating to him/her (in particular success at work, credit rating, reliability, handling or compliance with conditions required), shall only be permitted if the decision:

(i). is taken during the conclusion or implementation of a contract, provided that the request to conclude or implement a contract submitted by the individual to whom the personal data relate has been fulfilled or that there exist appropriate measures to protect his/her lawful interests, such as in particular agreements enabling him/her to object to such decision or to express his position; and

(ii) is provided by statute which also provides measures to protect the lawful interests of the individual to whom the personal data relate, particularly the possibility of legal remedy against such decision.

The data controller is on request of the individual obliged to explain to the individual the technical and logical-technical procedures of decision-making, if the controller is performing automated decision-making through the processing of personal data.

Please note that Slovenia has also ratified the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe of 1981.

## 13 Data Security and Data Breach

**13.1 What data security standards (e.g., encryption) are required, under applicable law or binding guidance issued by the relevant data protection authority(ies)?**

The PDPA does not explicitly regulate the level of the security standards for personal data protection. Under the law, the data controllers must comply with the general data security obligations and in addition prescribe in their internal acts the procedures and measures for security of personal data.

Security of personal data comprises of organisational, technical and logical-technical procedures and measures to protect personal data, and to prevent accidental or deliberate unauthorised destruction, modification or loss of data, and unauthorised processing of such data.

According to the PDPA, such security is provided:

- by protecting premises, equipment and systems software, including input-output units;
- by protecting software applications used to process personal data;
- by preventing unauthorised access to personal data during transmission thereof, including transmission via telecommunications means and networks;
- by ensuring effective methods of blocking, destruction, deletion or anonymisation of personal data; and
- by enabling subsequent determination of when individual personal data were entered into a filing system, used or otherwise processed, and who did so, for the period covered by statutory protection of the rights of an individual due to unauthorised supply or processing of personal data.

In cases of processing of personal data accessible over telecommunications means or networks, the hardware, systems software and software applications must ensure that the processing of personal data in filing systems is within the limits of authorisations of the data recipient.

The procedures and measures to protect personal data must be adequate in view of the risk posed by processing and the nature of the specific personal data being processed.

Functionaries, employees and other individuals performing work or tasks of persons that process personal data are bound to protect the secrecy of personal data with which they become familiar in performing their functions, work and tasks. The duty to protect the secrecy of personal data is also binding on them after termination of their function, work or tasks, or the performance of contractual processing services.

Further, in processing sensitive data, the data must be specially marked and protected to prevent unauthorised access. In the transmission of sensitive personal data over telecommunications networks, data is considered as suitably protected if it is sent using cryptographic methods and electronic signatures such that their illegibility or non-recognition is ensured during transmission.

**13.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.**

There is no explicit requirement to inform either the IC or the individual about the possible data breach.

Nevertheless, abuse of personal data is a criminal offence under the Article 143 of the Slovenian Penal Code (*Kazenski zakonik, KZ-1*). Whoever unlawfully uses personal data, which may be kept only on the basis of the law or on the basis of the personal consent of the individual, to whom the personal data relate, shall be punished by a fine or sentenced to imprisonment for not more than one year. The same applies for anyone who breaks into a computer database in order to acquire personal data for his/her or a third person's use. A special criminal offence is committed if someone publishes on the World Wide Web or enables another person to publish personal data of victims of criminal offences, victims of violation of rights and liberties, protected witnesses, which are contained in judicial records of court proceedings, in which the presence of the public or witness identification or protected witnesses and personal records thereof related to the court proceeding was not allowed according to the law or court decision, on the basis of which these persons may be identified or are identifiable. Assuming the identity of another person and exploiting under its name exploits their rights, gaining property benefits or damaging their personal dignity is also punishable.

As such, a voluntary reporting is expected in every case when a breach may be viewed as a criminal offence.

**13.3 Is there a legal requirement to report data breaches to individuals? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expects voluntary breach reporting.**

No; see question 13.3 above.

## 14 Enforcement and Sanctions

### 14.1 Describe the enforcement powers of the data protection authority(ies):

| Investigatory Power | Civil/administrative Sanction | Criminal Sanction |
|---|---|---|
| State prosecution: investigation of a criminal offence of abuse of personal data – general investigatory powers in a criminal procedure | No; eventual civil damages claim of an aggrieved individual | Fine punishment/ imprisonment for no more than one year |
| IC: supervision over the lawfulness of processing of personal data: supervising the implementation of the PDPA governing access to public information and regulations adopted within the framework of appellate proceedings – general inspection powers | Minor offence pecuniary fine; eventual civil damages claim of an aggrieved individual | There are no criminal sanctions |
| IC: supervision of the suit-ability of measures for security of personal data and the implementation of procedures and measures for security of personal data inspecting/supervising the implementation of the PDPA and other regulations, governing the protection or processing of personal data or transfer of personal data from Slovenia to third countries – general inspection powers | Minor offence pecuniary fine; eventual civil damages claim of an aggrieved individual | There are no criminal sanctions |
| IC: supervision of the implementation of the provisions of the statute regulating the filing system catalogue, the Register of Filing Systems and the recording of the supply of personal data to individual data recipients performing preventive supervision with personal data controllers in public and private sectors – general inspection powers | Minor offence pecuniary fine; eventual civil damages claim of an aggrieved individual | There are no criminal sanctions |
| IC: supervision of the implementation of the statutory provisions regarding the transfer of personal data to third countries and on the supply thereof to foreign data recipients – general inspection powers | Minor offence pecuniary fine; eventual civil damages claim of an aggrieved individual | There are no criminal sanctions |

### 14.2 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The Slovenian IC is very proactive in terms of issuing opinions, while it issues decisions only on rare and materially important occasions.

The opinions of the IC are predominantly of an informal nature. In these opinions the IC will give advice and direction that will not be binding (although may be taken into account in any future case).

Based on any form of the obtained information, the IC may ex officio initiate an inspection procedure with regard to the data controller concerning the implementation of the provisions of the PDPA. The IC usually primarily examines an eventual infringement, i.e. reviews the available evidence. The IC has the right to review documentation regarding the personal data regardless of its secrecy; it further has the right to inspect the rooms where the data is processed and to inspect the computers and other technical equipment. The IC further requests a written explanation on the implementation of the PDPA; the IC may even request for a temporary injunction with regard to an eventual personal data breach. IC further requests an explanation on the circumstances (statement) by the data controller and based on the conclusions issues a decision. No appeal is allowed against a decision; however an administrative dispute may be initiated within 30 days before the Administrative Court of the Republic of Slovenia.

The latest decision was issued in July 2012 (one of the two issued in 2012) and deals with the implementation of a web-based search engine of the Research Centre of the Slovenian Academy of Sciences and Arts, instructing the data controller to disable text search by name and family name of an individual.

## 15 E-discovery / disclosure to foreign law enforcement agencies

### 15.1 How do companies within Slovenia respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

There is no formal discovery process provided in Slovenia. The party needs to produce its own documents to support its case in the court proceeding. In this aspect the Slovenian law does not define any direct provisions regarding e-discovery. Provisions of the PDPA, the Slovenian Civil Procedure Act, provide that the Slovenian Criminal Procedure Act and the ECA should be noted in relation to the retention, preservation and transfer of the personal data as evidence or for use in possible further proceedings. E-discovery may be available under condition that the provisions of the PDPA are respected, i.e. having the sufficient legal base for obtaining such data, its processing and transfer.

### 15.2 What guidance has the data protection authority(ies) issued?

No relevant official guidance has been issued yet by the authorities. The Guidelines of the Data Protection Working Party set up under Article 29 of Directive 95/46/EC should be followed.

**Luka Fabiani**

CMS Reich-Rohrwig Hainz
Bleiweisova 30, 1000 Ljubljana
Slovenia

*Tel:* +386 1 620 5210
*Fax:* +386 1 620 5211
*Email:* luka.fabiani@cms-rrh.com
*URL:* www.cms-rrh.com

Luka Fabiani's focus is (Commercial) Dispute Resolution, Competition Law and Compliance (also White Collar Crime) and IP and IT law. He joined CMS after being a local partner an international business law firm for several years and continues to advise clients in litigation proceedings, as well as discretely and effectively defending clients in corporate criminal proceedings. He has been active for several clients in areas of competition law and compliance and IP and IT. He is fluent in Slovenian, English, German, Croatian and Serbian. He obtained his LL.M. (magister legum) in 2005 at the University of Tuebingen (Germany).

**Ela Omersa**

CMS Reich-Rohrwig Hainz
Bleiweisova 30, 1000 Ljubljana
Slovenia

*Tel:* + 386 1 620 5210
*Fax:* + 386 1 620 5211
*Email:* ela.omersa@cms-rrh.com
*URL:* www.cms-rrh.com

Ela Omersa joined CMS Reich-Rohrwig Hainz in January 2012. She graduated from the University of Ljubljana in 2010, spending an exchange year at Heidelberg University in Germany. During her studies she has been active in another Slovenian law firm, where she gained experiences in the field of employment law, civil law, social security law and corporate law. She has recently obtained an LL.M. degree at the University of Utrecht (The Netherlands) and later started to work as an associate with an international law office in Ljubljana, before joining the CMS team. She is volunteering at the High Court in Ljubljana. Ela speaks Slovenian, English and German.