PrivacyRules Country Overview: Privacy and Data Protection in Slovakia

Mgr. Michal Nulíček, LL.M., CIPP/E

Michal Nulíček focuses in his practice on data and privacy protection, regulation on consumer protection, whistleblowing as well as on commercial, IT, IP, and competition law.

He acted as a leading advisor on various GDPR implementation projects for leading Czech and international companies. Michal also advises clients in connection with raids conducted by the Czech Data Protection Office, assists them in dealing with the Czech authorities and conducts seminars for clients on data protection and regulatory compliance.

Contact details:
Email: nulicek@rowan.legal
Phone number: 00 420 224 216 212
Cell phone: 00 420 224 216 212
Fax: 00 420 224 215 823

*[**SCOPE:** The scope of the Country Overview template is to confirm to clients the quality and accuracy of the expertise that PrivacyRules and its Members can provide. It is an informative document, yet does not constitute advise or give direction on the design of privacy policies in each given jurisdiction]*

*[**COMPILATION:** Simple yes / no answer, brief explanation (limited to max 5 lines per answer) with indication of title and year of adoption when referring to laws / bills / regulations / guidelines, list the latest one first. This information will be reproduced on the PrivacyRules webpage under "The law of privacy"]*

Q: Are privacy and data protection recognised by the Constitution / Fundamental Rights Bill?

A: Yes, according to the Constitution, the inviolability of the person and his or her privacy is guaranteed (Art. 19 (2)), everyone has the right to be protected from the unauthorized gathering, public revelation, or other misuse of her personal data (Art. 19 (3)) and to the secrecy of correspondence (Art. 22).

Q: Is there primary legislation on privacy, data protection, cybersecurity, cybercrime, cyberterrorism?

A: Yes, the right to privacy is laid down by Act no. 19/1964 Coll., Civil Code. The main data protection law in Slovakia that implements GDPR is Act no. 18/2018 Coll., on Personal Data Protection. The cybersecurity regulation is provided in Act no. 69/2018 Coll., on Cyber Security. Cybercrimes as well as other crimes are generally contained in Act no. 300/2005 Coll., Penal Code.

Q: What are the fields of law closely related to privacy and data protection that are regulated in the Slovakian jurisdiction? (e.g. e-commerce, telecommunications, media, intellectual property, etc.).

A: Yes. Act no. 351/2011 Coll., Electronic Communications Act that regulates electronic communication. Act no. 22/2004 Coll., on E-Commerce that regulates commercial communications.

Q: What are the key definitions in the field of data protection (e.g. Personal Data, Sensitive Data, Data Processing, Data Controller, Data Subject, Pseudonymised Data, Anonymised Data, Processing or any other definition)?

A: The key definitions are same as in Art. 4 GDPR.

Q: In particular, is there a distinction between identifiable, pseudonymised and anonymised data and if so, how are they regulated?

A: Yes, the same as in GDPR. The legal distinction between anonymised and pseudonymised data is its categorisation as personal data. Pseudonymous data still allows for some form of re-identification (even indirect and remote), while anonymous data do not allow such re-identification.

Q: Is there a national Data Protection Authority?

A: Yes, the Office for Personal Data Protection (in Slovak: Úrad na ochranu osobných údajov – https://dataprotection.gov.sk/uoou/)

Q: Which national judicial authorities are competent on privacy and data protection related matters?

A: In general, there is no special judicial authority competent on privacy and data protection related matters. Therefore, district courts are competent in the first instance. However, the administrative chamber within a regional court acts as a court of the first instance in case the final decision of the Slovak Office for Personal Data Protection is challenged.

Q: Is there a one-stop-shop mechanism in place?

A: Yes, in line with GDPR.

Q: What are the main enforcement measures?

A: The Slovak Data Protection Office is authorized to perform inspections of data processing activities and following that issue an injunction or decision with the imposition of administrative fine and prohibition of activities against data protection regulation.

Q: What are the actual main sanctions?

A: Administrative fine (the highest fine is 50 000 EUR), injunction leading to the cease of specific data processing activities or erasure of personal data.

Q: Is there a supra-national applicable legal framework? If the answer is positive, is it binding and to what extent?

A: Yes, GDPR – Regulation (EU) 2016/679 of the European Parliament And of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Q: Does any foreign authority have jurisdiction on privacy and data protection matters for citizens of Slovakia? If the answer is positive, do they have executive or advisory authority?

A: The Court of Justice of the European Union (CJEU) is the authority that interprets the European laws and national courts of EU countries are required to ensure EU law is properly applied in accordance with binding decisions of CJEU.

Q: Are there e-discovery or disclosure duties pursuant to a request from a foreign Law Enforcement Agency?

A: The limits of the duty to disclose data on request of foreign Law Enforcement Agencies are laid down by Art. 48 GDPR. According to that a request must be based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State.

Q: Are privacy-by-design and privacy-by-default mandatory?

A: Yes, pursuant to Art. 25 GDPR.

Q: Are data protection officers (DPOs) foreseen by law and if so, to what extent?

A: Yes, DPOs are foreseen by Art. 37 GDPR. According to that, the DPO shall be designated in any case where:

a) *the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;*
b) *the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or*
c) *the core activities of the controller or the processor consist of processing on a large scale of special categories of data;*

Q: Are data protection impact assessments (DPIAs) mandatory and if so, to what extent?

A: Yes, DPIAs are mandatory in cases stipulated by Art. 35 GDPR (e.g. systematic and extensive evaluation of personal aspects, processing on a large scale of special categories of data, systematic monitoring of a publicly accessible area on a large scale).

Q: Is there any obligation to register databases and if so, to what extent?

A: No registration of databases is required under Slovak data protection laws.

Q: Are definitions like controller, processor, regulator clearly defined and identifiable within the Slovak regulatory framework?

A: The definitions are contained in Art. 4 GDPR.

Q: Are there obligations to adopt reasonable technical, physical and organizational measures to protect the security of sensitive personal information and if so, to what extent?

A: Yes, according to Art. 32 GDPR the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Q: Are there security breach notification requirements and if so, to what extent?

A: Yes, a personal data breach must be notified to the relevant supervisory authority unless it is unlikely to result in a risk to data subjects. The notification must, where feasible, be made within 72 hours. If the personal data breach is a high risk for data subjects, those data subjects must also be notified.

Q: Can authorities access large amounts of data and/or specific data without a court or prosecutor's order?

A: Yes, if such data processing is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest. However, in some cases, a court's order is necessary, e.g. when law enforcement bodies and intelligence agencies request operating and location data from ISP and telecommunication providers.

Q: Are there specific kinds of data covered by stronger provisions on legal protection (e.g. children data, etc.)?

A: Yes, there are special categories of personal data, e.g. genetic data, biometric data, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership. According to GDPR, there are also provisions that strengthen the regulation of the processing of personal data of children.

Q: Is there a specific regulation for the collection of data?

A: Yes, every data collecting activity shall be based on legal grounded stipulated by Art. 6 GDPR and respect the general data protection principles provided in Art. 5 GDPR.

Q: Is it possible to use personal data for electronic marketing purposes and if so, to what extent?

A: The controller is entitled to use personal data collected from data subjects to direct marketing purposes. However, a data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing.

Other marketing activities, e.g. such activities of third parties, typically require prior consent to be given by data subject.

Q: Is transfer of data outside the Slovak jurisdiction regulated?

A: Not outside the Slovak jurisdiction but outside the European Union. According to GDPR, personal data may be transferred to a third country outside the EU only if:

a) *the European Commission decided that such third country ensures an adequate level of protection;*
b) *the controller or processor has provided appropriate safeguards in line with Art. 46 GDPR (e.g. conclusion of standard contractual clauses between a data exporter and a data importer, binding corporate rules);*
c) *derogations for specific under Art. 49 GDPR applies.*

Q: Can individuals access their data and request their correction or deletion?

A: Yes, exercise of those rights is regulated by Articles 15 and 17 GDPR.

Q: How can individuals exercise their privacy rights?

A: Individuals may lodge a complaint to the Slovak Office for Personal Data Protection or file a legal action before a competent court.

Q: Are there associations entitled to advocate privacy and data protection rights?

A: No

Q: Is access to data regulated according to specific and detailed legal acts stating legal requirements to exercise the right to access, e.g. timeframe, identity and categories of legitimate applicant, templates for various forms of request, obligations of the requested entity etc.?

A: Yes, the right to access is regulated by Article 15 of the GDPR. However, there are few limitations regarding this right that applies according to Act no. 18/2018, on Personal Data Protection, only to processing that is necessary for compliance with a legal obligation to which the controller is subject or that is necessary for the performance of a task carried out in the public interest.

Miscellaneous: Any other information particularly important in Slovakia jurisdiction [if necessary, please explain why this additional information is provided and which is its relevance].

A: N/A
