Client Alert

Slovenia's New Data Protection Act - fines, traceability logs and much more

Start 2023 with sound data protection compliance

29 December 2022

After a more than 4-year delay, Slovenia has finally adopted the new Data Protection Act[1] ("DPA"), which will apply as of 26 January 2023 and replace the existing Data Protection Act from 2004

Under the new DPA, the Slovenian Information Commissioner will now have the authority to impose fines pursuant to the General Data Protection Regulation ("GDPR"). More than 100 articles of the new DPA also introduce several new rules.

The new DPA brings about not only the derogation provisions of the GDPR but also introduces rules on the age limit for a child's consent, processing for the purpose of scientific research, use of CCTV and biometric data and certain additional security obligations to be ensured by the companies carrying out processing of personal data on a large scale.

The following provisions are particularly noteworthy and will be described in more detail below:

- response to a data subject's request;
- additional security obligations;
- age limit for a child's consent;
- processing of publicly available contact details; and
- fines for non-compliance.

> The new DPA covers much more than just the derogation provisions of the GDPR.

[1] Data Protection Act (*Zakon o varstvu osebnih podatkov – ZVOP-2*), Official Gazette of RS, no. 163/2022.

Response to a data subject's request

In addition to the GDPR's requirements, the DPA specifies that a response to a data subject's request must include a justification and the information on the data subject's right to lodge a complaint with the supervisory authority (i.e. the Information Commissioner) within 15 days from acknowledgment of the respective response. This applies to a data subject's request regarding her/his rights pursuant to Art. 15 – 22 of the GDPR[2] as well as any other requests related to the protection of personal data. All such responses must be provided free of charge.

For manifestly unfounded or excessive requests, the data controller may charge a reasonable fee. However, such fee may only include the actual costs of providing the information, response, communication or actions.

Additional security obligations

The new DPA introduces two additional security obligations: (i) administration of a traceability log and (ii) security of special processing activities. Both obligations will likely present a significant burden for companies, but these requirements will not become applicable in 2023, giving businesses some time to prepare. The obligation regarding the traceability logs will apply only from the second anniversary of application of the DPA (26 January 2025). The obligation concerning security of special processing activities will apply only from the third anniversary of application of the DPA (26 January 2026).

Special **traceability logs** will have to be administered by those data controllers who (i) carry out data processing of special categories of personal data on a large scale, or (ii) carry out regular and systematic monitoring of individuals, or (iii) in the context of data protection impact assessments, determine a risk which can be successfully mitigated with traceability logs, or (iv) in other instances if determined by law. The logs are to be used for accountability and internal audit purposes.

The traceability logs must record collection, change, access, disclosure, deletion and other processing activities determined by law. The traceability logs must be retained for a period of 2 years following the end of a calendar year in which they were recorded.

The **security of special processing activities** in certain information systems must not only be ensured in line with the GDPR, but also with security and incident reporting measures under the Slovenian Information Security Act[3] (*Zakon o informacijski varnosti – ZinfV;* "**Information Security Act**") (the act implementing the NIS Directive[4]), which is otherwise applicable to operators of essential services and key digital service providers.

Subject to these additional security obligations under the Information Security Act are information systems, used for the processing of:

- personal data of more than 100,000 individuals on the basis of the law; or
- personal data of special categories of personal data on a large scale by processors or controllers, which carry out such processing as their main business operation; or
- special categories of personal data of more than 10,000 individuals.

---

[2] Right to access, right to rectification and erasure, right to restriction of processing, right to data portability, right to object.

[3] Information Security Act (*Zakon o informacijski varnosti – ZInfV*), Official Gazette of RS, no. 30/18, as subsequently amended.

[4] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30

Age limit for a child's consent

In relation to the offer of information society services[5] directly to a child, the DPA sets the age limit for a valid child's consent for processing of his/her personal data at 15 years. If a higher age limit is determined in the terms of use of a service provider, such higher age limit prevails over the statutory age limit.

Use of publicly available personal data

The new DPA introduces two exceptions for the use of personal data collected from public sources or events:

- a company may use contact details collected from public sources or disclosed to it by individuals voluntarily or on the basis of consent for the purposes of organising official meetings, trainings, events, and providing public statements. Use for the purpose of direct marketing is excluded. Such personal data must be kept separately from other personal data held by the company.
- for the purpose of publications, a company may process and publish the name, title, photos and videos of individuals obtained during events, which are organised by such company in the course of its operations, provided that an individual did not prohibit such processing.

Fines for infringements

One of the most notable provisions to be introduced by the new DPA is the possibility for the Slovenian Information Commissioner to impose fines under the GDPR for infringements of the GDPR and the new DPA. Up until the applicability of the new DPA, the Information Commissioner could only impose fines for infringements under the existing Data Protection Act (ZVOP-1). Such fines were rather low and ranged from EUR 4,170 to EUR 12,510.

However, fines under the GDPR will not be imposed in the following cases:

- offence proceedings started prior to the applicability of the new DPA will end under the provisions of the existing Data Protection Act (ZVOP-1), unless the new DPA is more lenient for the infringing company. On the other hand, the ongoing inspection proceedings will continue in line with the new DPA;
- for infringements committed prior to the applicability of new DPA, the fines as determined under the GDPR will apply only if the GDPR can be considered the most lenient law for the infringing company as compared to other laws applicable since the date of infringement.

[5] The DPA introduces a definition of "information society services", and this means any service normally provided for remuneration, at a distance (service is provided without the parties being simultaneously present), by electronic means (service is sent initially and received at its destination by means of electronic equipment for the processing and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means) and at the individual request of a recipient of services (the service is provided through the transmission of data on an individual request). The definition is aligned with the definition of information society service under the Directive (EU) 2015/1535.

The table below shows the range of fines under the new DPA and the GDPR.

Infringement	Company	Responsible person of a company
• breach of the obligations of the controller and the processor (Art. 8, 11, 25 to 39 and 42 and 43 of GDPR).	up to EUR 10 million or 2 % of the annual turnover, whichever is higher[6]	EUR 100 to EUR 5,000
• breach of the provisions on the basic principles for processing, including conditions for consent (Art. 5, 6, 7 and 9 of GDPR); • breach of the data subjects' rights (Art. 12 to 22 of GDPR); • breach with respect to the transfers of personal data (Art. 44 to 49 of GDPR).	up to EUR 20 million or 4 % of the annual turnover, whichever is higher[7]	EUR 200 to EUR 8,000
• breach with respect to the administration of a traceability log and security of special processing activities (Art. 22 and 23 of DPA)	EUR 8,000 to EUR 36,000 (medium and large companies) EUR 4,000 to EUR 12,000 (other companies)	EUR 400 to EUR 4,000
• breach of the general CCTV obligations (Art. 76 of DPA)	EUR 8,000 to EUR 20,000 (medium and large companies) EUR 4,000 to EUR 10,000 (other companies)	EUR 500 to EUR 2,000

* * *

Should you require any further details regarding the new legislative changes and how to effectively ensure compliance with them, please do not hesitate to contact us.

[6] The annual turnover refers to the total worldwide annual turnover of the preceding financial year of an undertaking pursuant to Art. 83 of GDPR.

[7] Ibid.

About Wolf Theiss

Wolf Theiss is one of the leading European law firms in Central, Eastern and South-Eastern Europe with a focus on international business law. With more than 360 lawyers in 13 countries, over 80% of the firm's work involves cross-border representation of international clients. Combining expertise in law and business, Wolf Theiss develops innovative solutions that integrate legal, financial and business know-how.

For more information, please contact:

Klemen Radosavljević
Partner

E klemen.radosavljevic@wolftheiss.com
T +386 1 438 0023

Larisa Primožič
Associate

E larisa.primozic@wolftheiss.com
T +386 1 438 0020