LAW


North Macedonia expects to adopt a new data protection law in 2019 to align with the EU General Data Protection Regulation (GDPR).

DEFINITIONS

Definition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural entity, where an identifiable entity is an entity whose identity can be especially determined, directly or indirectly, on the basis of his or her personal identification number or on one or a combination of features that are specific to his or her physical, mental, economic, cultural or social identity.

Definition of sensitive personal data

Under the DP Law, sensitive personal data is personal data related to:

- Racial or ethnic origin
- Political or religious views, or other beliefs
- Membership in a trade union
- Health, including genetic data, biometric data and data referring to sexual life

NATIONAL DATA PROTECTION AUTHORITY

The Directorate for Personal Data Protection (DPA) was established in 2005 as North Macedonia’s data protection authority. The DPA is an independent state agency with competence to oversee DP Law implementation, with its registered seat located at:

Bulevar Goce Delcev 8
Skopje
www.dlzp.mk

REGISTRATION

Any natural or legal entity who intends to collect, process or maintain a database containing personal data (Database) in North
Macedonia must notify the DPA prior to the commencement of any such activity.

This requirement does not apply to entities that:

- Have fewer than 10 employees
- Intend to process publicly available personal data
- Intend to process personal data of members of nonprofit organizations that are established for political, philosophical, religious or trade-union purposes

Entities must register (1) themselves as data controllers, and (2) their respective Databases with the DPA’s Central Register of Databases. Data controllers must provide all relevant information on particular data processing activities, including: corporate details, types of data processed, purpose of processing, data retention periods, legal grounds for Database establishment, personal data transfers to other countries, and security measures in place to protect data integrity.

To register, entities must complete an online form: www.dzlp.mk. The DPA requires entities to report subsequent changes to registration details within 30 days of a change.

DATA PROTECTION OFFICERS

Under the DP Law, data controllers subject to registration requirements (see Registration section above) must appoint a data protection officer tasked with ensuring data controller compliance with the DP Law and other applicable regulations.

Data protection officers must:

- Participate in all decisions related to personal data processing and data subject rights over their personal data
- Prepare corporate by-laws on personal data protection, including technical and organizational measures designed to protect personal data and maintain its confidentiality
- Monitor data controller compliance with the DP Law and related regulations, specifically as relates to the corporate by-laws on personal data protection
- Coordinate internal personal data protection procedures and guidelines, and
- Develop data controller employee training on personal data protection

COLLECTION & PROCESSING

The DP Law sets forth the fundamental principles for personal data collection and processing require, which require that data controllers collect and process personal data:

- Fairly and lawfully
- For legitimate purposes
- Proportionally to the needs for collection and processing
- Accurately and completely, and
- To store data in a manner that enables data subject identification

Data controllers must obtain data subjects informed consent prior to personal data collection or processing, including as relates to personal identification numbers and sensitive personal data. Informed consent requires data controllers provide data subjects with all relevant information on personal data processing and collection, such as the purpose of processing, data subject rights, retention policy, and data transfers.

Exceptions to informed consent requirements permit data controllers to collect and process personal data without data subject consent to protect data subject life or vital interests, to protect public interests or to exercise the legitimate rights of the data controller, unless such processing or collection is in conflict with data subject fundamental rights and freedoms.
TRANSFER

Entities may only transfer personal data outside of North Macedonia to countries where adequate personal data protection levels apply. The DPA has authority to assess third country personal data protection levels and approve personal data transfers outside of North Macedonia.

Entities are not required to obtain DPA approval for personal data transfers to European Union (EU) and European Economic Area (EEA) countries, as the DP Law creates a legal assumption that EU and EEA countries provide adequate personal data protection levels.

Entities must obtain DPA approval for transfers to non-EU/EEA countries “white-listed” by the EC as providing adequate data protection levels, though through a simplified DPA approval process. The DPA relies on European Commission (EC) assessments of non-EU/EEA country personal data protection levels.

Personal data transfers outside of North Macedonia are prohibited, without the consent of the DPA, to third countries that the EC has not found to provide adequate data protection levels. Absent an EC adequacy determination, the DPA is required to assess and approve personal data transfers to non-EU/EEA countries. Minimal guidance exists on the DPA assessment and approval approach. Under the DP Law, DPA assessments should consider:

- The nature of the data
- The purpose and duration of the proposed processing
- Governing law in the country where the data is to be transferred, and
- Protective measures existing in the respective country

1: Andorra, Argentina, Australia, Canada (commercial organisations), Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Uruguay and the US (only companies that are compliant with the Department of Commerce’s Safe Harbour Privacy Principles).

SECURITY

The DP Law requires data controllers and processors to implement appropriate technical and organizational measures to protect personal data from accidental or illegal damage, illegal processing, accidental loss, change, unauthorized access or disclosure, and particularly as relates to processing that includes data transmission over a network. However, the DP Law does not require use of a specific technology to protect personal data.

Technical and organizational measures should be proportional to the risk posed by a breach to the integrity of data, considering the nature of the data being processed. The DP Law provides guidance to establish three personal data protection levels by using a combination of technical and organizational measures:

1. Basic
2. Medium
3. High

Data controllers and processors are required to adopt internal regulations (ie, corporate by-laws) with a description of technical and organizational measures for personal data protection.

BREACH NOTIFICATION

Under the DP Law, data controllers and processors are not required to report data security breaches to the DPA. The DPA is unable to trace data security breaches unless a data subject reports a breach of his or her rights, or through a random inspection of a data controller and processor.
ENFORCEMENT

The DPA has DP Law enforcement and oversight authority, and may monitor DP Law compliance through random data controller and processor inspections, or upon receipt of a data subject complaint.

The DPA enforces DP Law violations by ordering data controllers or processors to remedy violations within a specified time period, or by imposing a fine, taking the seriousness of the offense into consideration. Legal entity fines range from €1,000 to €2,000 per violation. Additionally, the DPA may issue a fine to the responsible person within the legal entity in an amount equal to 30% of the fine imposed on the legal entity. Entities may dispute DPA fines by initiating proceedings before the Administrative Court.

The DPA may further require data controllers or processors in violation of the DP Law to attend mandatory training on data protection issues organized by the DPA.

The Macedonian Criminal Code includes a criminal offense for misuse of personal data punishable by a monetary fine or imprisonment of up to one year, as determined by the court.

ELECTRONIC MARKETING

Under the DP Law, personal data may be processed for electronic marketing purposes only with the data subject explicit consent to such processing, provided that the data subject is entitled to withdraw his or her consent at any time free of charge.

ONLINE PRIVACY

There are no specific regulations governing online privacy, including cookies. However, general data protection rules under the DP Law apply to the extent possible.

KEY CONTACTS

Ljupka Noveska Andonova
Senior Associate
Karanovic & Partners
T +389 2 3223 870
ljupka.noveska@karanovicpartners.com

DATA PRIVACY TOOL

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

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.