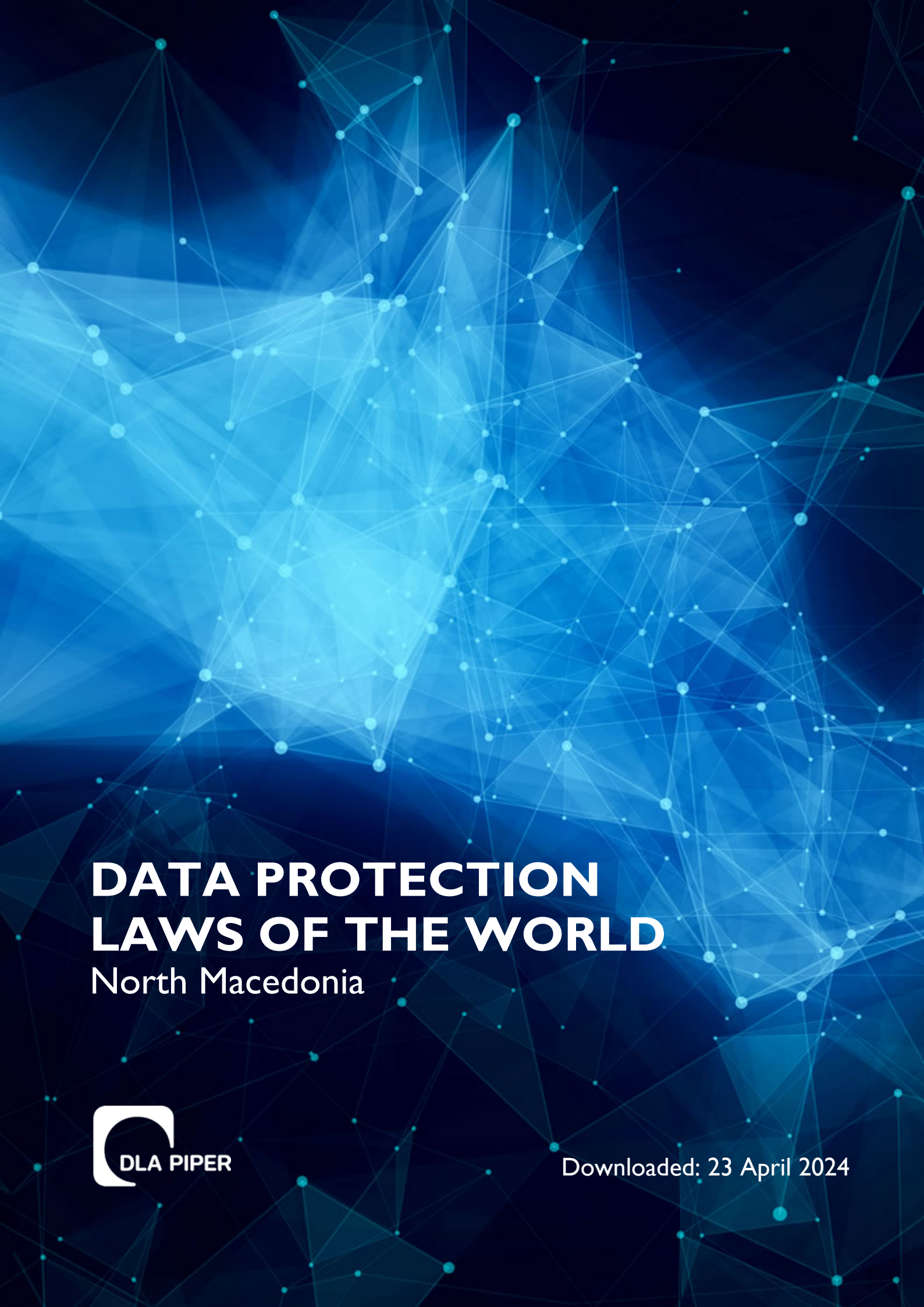

DATA PROTECTION LAWS OF THE WORLD

North Macedonia

DLA PIPER

NORTH MACEDONIA

Last modified 17 January 2024

LAW

The Republic of North Macedonia regulates personal data protection issues with the Law on Personal Data Protection (Official Gazette of the Republic of North Macedonia, no. 42/20 and 294/21, “**DP Law**”), effective 24 February 2020. Data controllers and data processors had an 18-month period from the DP Law’s entry into force (i.e. until 24 August 2021) to harmonize their operations with the DP Law. This period has been informally prolonged for additional six months, during which time the data protection authority assisted companies in the implementation of the new rules through education and corrective measures, as opposed to directly issuing fines for non-compliance.

The DP Law is largely harmonized with the General Data Protection Regulation (GDPR) of the European Union (EU).

DEFINITIONS

Definition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural person, where an identifiable natural person is one whose identity can be determined directly or indirectly, especially by reference to an identifier such as a name and surname, his or her personal identification number, location data, an online identifier or on one or a combination of features that are specific to his or her physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Definition of sensitive personal data

Under the DP Law, sensitive personal data is personal data which reveal:

- racial or ethnic origin;
- political opinions, religious or philosophical beliefs;
- membership in a trade union;
- genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data referring to a natural person’s sex life or sexual orientation.

NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Agency (“**DPA**”) was established in 2005 with the Law on Protection of Personal Data dated 2005 (then called the Directorate for Personal Data Protection of the Republic of Macedonia, while with the adoption of the DP Law it became an agency) as North Macedonia’s data protection authority. The DPA is an independent state agency with competence to oversee the implementation of the DP Law, with its registered seat located at:

Boulevard Goce Delcev 18

1000 Skopje, Republic of North Macedonia

Website

azlp.mk

REGISTRATION

The DPA keeps records of all data controllers and data protection officers and publishes them on its website.

Under the Law on Protection of Personal Data dated 2005, data controllers / processors had an obligation to register their databases containing personal data in the Central Registry of Personal Databases (“**Registry**”) maintained by the DPA. With the adoption of the DP Law, this Registry changes in a way that it continues to exist, i.e. continues to be maintained by the DPA, but as a registry of databases involving a high risk (“**High-Risk Records**”), whereas controllers / processors should notify the DPA about their respective high risk databases. It is also envisaged that the provisions of the DP Law governing the High-Risk Records shall cease to apply upon accession of the Republic of North Macedonia to the EU.

The DPA requires entities to report subsequent changes to registration details within 30 days of a change.

The DP Law obliges data controllers / processors and their representatives to maintain records of processing activities with an explicitly prescribed content. However, this obligation is not an obligation generally applicable to all data controllers and data processors. It applies only if data controllers / processors have at least 50 employees or, regardless of their employees’ number, if the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of personal data or personal data relating to criminal convictions and offences.

DATA PROTECTION OFFICERS

Under the DP Law, data controllers and data processors are obliged to appoint a DPO in certain cases, i.e. when:

- processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
- core activities of the data controller/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
- core activities of the data controller/processor consist of processing on a large scale of special categories of personal data and personal data relating to criminal convictions and offences.

Data protection officers must:

- inform and advise the data controller or data processor and employees who process data about their duties in accordance with the DP Law;
- monitor compliance with the DP Law, with other national laws and with the policies of the controller/processor;
- increase awareness of data protection practices;
- provide advice on Data Protection Impact Assessment;
- collaborate with the DPA;
- act as a contact for the DPA regarding the adequate collection and processing of personal data and perform other prescribed tasks.

COLLECTION & PROCESSING

The DP Law operates on the basis of the principles of lawfulness, fairness and transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality and accountability.

The requirement of carrying out the data processing lawfully means that, amongst other, it should be based upon adequate legal ground. Such legal ground is either a data subject's consent (relating to specified, explicit and legitimate purpose/-s) or one of the remaining grounds explicitly prescribed by the DP Law which include:

- necessity of a particular processing for the performance of a contract to which a data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- necessity for compliance with a legal obligation to which the data controller is subject;
- necessity for the protection of the vital interests of the data subject or of another natural person;
- necessity for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller, and
- necessity for realization of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.

The processing of special categories of personal data is prohibited, unless an exception prescribed with the DP Law applies.

Data subjects are entitled to a range of rights under the DP Law, including right of access, right to rectify, right to erasure (‘right to be forgotten’), right to restriction of processing, right to data portability, right to object, right not to be subject to automated decision making, including profiling.

TRANSFER

Entities may transfer personal data which are subject to processing if the conditions set out in the DP Law are fulfilled and applied.

When transferring personal data to the EU or the European Economic Area (EEA), entities must notify the DPA at least 15 days before the transfer.

Transferring personal data to third countries or international organizations may be conducted only if the DPA deems that the third country or international organization provides adequate levels of protection. When assessing whether the third country or international organization has an adequate level of protection, the DPA considers several parameters, including, among others:

- the rule of law, respect for human rights and fundamental freedoms, relevant legislation and its implementation, professional rules and security measures (including rules for onward transfer), as well as effective and enforceable judgements applied to data subject and effective and administrative and judicial redress for data subjects whose personal data is transferred;
- the existence and effective functioning of one or more independent supervisory authorities in the third country or international organization;
- the international commitments the third country or international organization has entered into, or other obligations arising from legally binding conventions or instruments, in relation to the protection of personal data.

If the above criteria are met by the third country or international organization where the personal data will be transferred, the data transfer can be conducted on the basis of an adequacy decision adopted by the DPA.

The DPA has not yet adopted an adequacy decision. However, the DPA follows the practice of the European Union when it comes to implementing the data protection regulations, and it is expected that any such adequacy decision will be in line with an adequacy decision adopted by the European Commission.

The DP Law itself does not require a special / individual prior approval by the DPA (“**Transfer Approval**”) if an

adequacy decision issued by the DPA for the (importing) third country or international organization exists or the below safeguards are provided (on condition that enforceable data subject rights and effective legal remedies for data subjects are available). However, up until this point in time, the DPA has had a conservative approach.

When an adequacy decision has not been adopted, personal data can be transferred to a third country or international organization only if the data controller or data processor apply appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The appropriate safeguards may be provided by:

- a legally binding and enforceable instrument between public authorities or bodies;
- binding corporate rules in accordance with the DP Law;
- standard data protection clauses determined by the DPA or approved by the European Commission;
- an approved code of conduct or approved certification mechanism pursuant to the DP Law together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards the data subjects’ rights.

Additionally, the DPA could approve the following appropriate safeguards:

- contractual clauses between the data controller and the data processor, as well as the data controller, the data processor or the recipient of the personal data in the third country or international organization; or
- provisions envisaged in administrative agreements between public authorities or bodies which contain applicable and effective data subject rights.

The DP Law also provides a list of derogations for specific situations, based on which a legitimate data transfer out of the Republic of North Macedonia is not conditioned upon a Transfer Approval (e.g. data subject’s consent, enforcement of a contract between a data subject and a data controller, etc.).

Unofficially, starting from 2022, the DPA requires the submission of a performed transfer impact assessment with each request for Transfer Approval when transferring personal data to third countries and international organizations.

Even if the requirements to submit a request for Transfer Approval are not met, but the cross-border transfer of personal data is based on other bases, controllers / processors should still perform a documented transfer impact assessment.

SECURITY

The DP Law requires data controllers and data processors to implement appropriate technical and organizational measures to protect personal data from accidental or illegal destruction, loss, alteration, unauthorized disclosure of personal data or unauthorized access to transferred, stored or otherwise processed personal data. These risks are particularly taken into consideration in order to assess the appropriate level of safety.

The technical and organizational measures include, *inter alia,* as appropriate:

- the pseudonymization and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

The data controller and the data processor must always implement the technical and organizational measures relevant to the period in which they are designed and implemented, in accordance with the state-of-the-art technology.

The data controller and the data processor are obliged to apply appropriate levels of technical and organizational measures proportional to the processing activities, while taking into consideration the nature, scope, context and purposes of the processing, as well as the risks with different probability and seriousness for the rights and freedoms of natural persons.

The technical and organizational measures can be classified in two levels:

1. Standard; and
2. High.

The process for managing the system for personal data protection is described in the internally adopted Policy on the System for Personal Data Protection, which should be regularly updated and harmonized in line with any changes in the data controller’s working process.

BREACH NOTIFICATION

Under the DP Law, data controllers are obliged to immediately (and not longer than 72 hours after discovering the data breach) inform the DPA, unless it is likely that the data breach may not pose a risk to the rights and freedoms of natural persons. Data processors are obliged to notify the data controller immediately after discovering the breach.

The notification is submitted on a special form prescribed by the DPA. The information may be gradually submitted without undue delays, only if there was no possibility to submit all of the information at the same time.

If the data breach is deemed to pose a high risk to the rights and freedoms of the natural persons, the data controller must immediately notify the data subject that their personal data has been breached. However, the data controller may not notify the data subject if:

- appropriate technical and organizational measures have been implemented which ensure that the personal data would be unrecognizable to unauthorized persons (e.g. encryption);
- the data controller has implemented additional measures which ensure that there is no longer a high risk to the rights and freedoms of the data subjects; or
- if such notification requires disproportionate effort, in which case a public notification or a similar measure is implemented.

ENFORCEMENT

The DPA has supervisory authority over the protection of personal data, as a systemic and independent control over the legality of the undertaken actions during personal data processing. This supervision entails the inspection, assessment, giving direction and imposing measures to data controllers and processors, through supervisors with the DPA.

The supervision may be:

- regular (announced supervision, conducted in line with the DPA’s annual supervision program);
- extraordinary (unannounced supervision, conducted upon a request, initiative, ex officio or in cases where the supervisors suspect that a breach of the DP Law has occurred); and
- control (conducted within six months after the expiration of the deadline for rectifying violations).

The supervisors enforce DP Law violations by ordering data controllers or processors to remedy violations within a specified time period, or by requesting the initiation of a misdemeanor procedure before the Misdemeanor Commission, taking the seriousness of the offense into consideration. Legal entity fines range from up to 2% and up to 4% of the total annual turnover from the previous financial year, with smaller fines of several hundred euros for the responsible persons at the infringer and the data

controllers and processors who are natural persons. Additionally, there is a fine in the range between EUR 1,000 to EUR 10,000 for data controllers which are legal entities who do not adhere to the video surveillance requirements. Entities may dispute DPA fines by initiating proceedings before the Administrative Court of the Republic of North Macedonia.

Individuals are also entitled to bring private claims against controllers and/or processors and request compensation of material or non-material damages suffered due to a breach of the DP Law. Individuals also have the right to lodge a complaint to the DPA and right to an effective judicial remedy against a decision (or lack of) of the DPA concerning them.

The Criminal Code of North Macedonia 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 (direct) marketing purposes including profiling to the extent connected to the direct marketing only with the data subject’s explicit consent to such processing. The data subject has the right to withdraw his or her consent at any time.

The data subject is entitled to exercise his or her right to object at any time to processing of his or her personal data for such marketing. In situations where the data subject objects to the processing, the personal data shall no longer be processed for such purposes.

ONLINE PRIVACY

The DP Law and the Rulebook on the Security of Personal Data Processing (Official Gazette of the Republic of North Macedonia no. 122/20, **“Security Rulebook”**) apply to online privacy as well.

In line with the Security Rulebook, when using cookies which are not necessary from the service, the data controller should obtain previous consent from the internet user before the cookie is deposited. Data subjects should be informed about the use of cookies and their type, duration, provider, purpose, with which third parties the data is shared, as well as the manner in which cookies can be rejected.

Please note that data controllers and data processors should undertake technical and organizational measures for security of the personal data processing to guarantee the correct identity of the website, as well as the confidentiality of the sent and received information, as prescribed with the Security Rulebook. For example, this would include mandatory use of cryptographic protocol (TLS) for all pages of the website, adoption of a policy for the personal data protection system, etc.

KEY CONTACTS

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

Veton Qoku
Partner
Karanovic & Partners
T +389 2 3223 870
veton.qoku@karanovicpartners.com

Ana Kashirska
Senior Associate
Karanovic & Partners
T +389 2 3440 682
ana.kashirska@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.