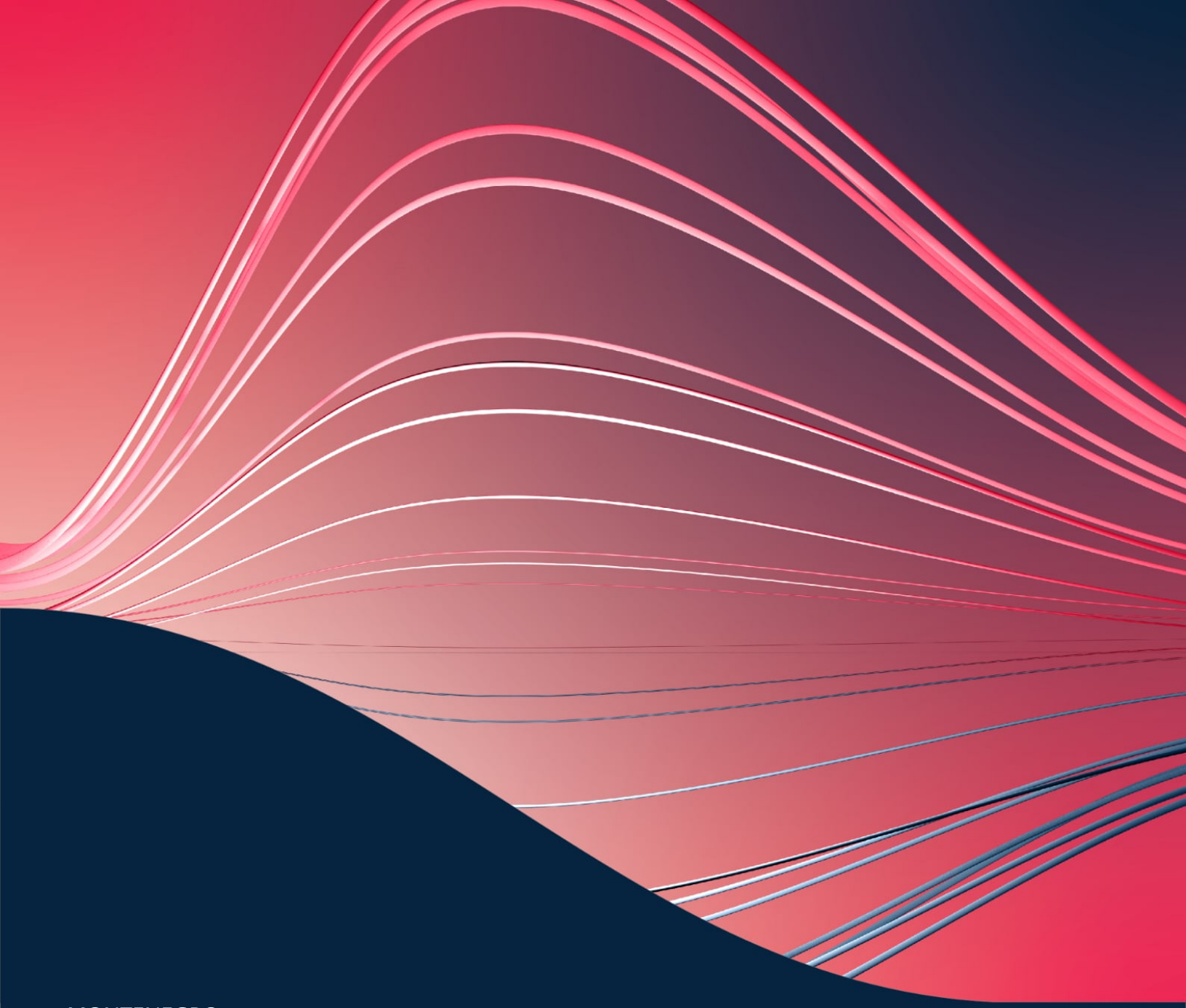


MONTENEGRO

Data Protection Laws of the World

DLA PIPER

Introduction

Welcome to the 2025 edition of DLA Piper's Data Protection Laws of the World Handbook. Since the launch of our first edition in 2012, this comprehensive guide has been a trusted resource for navigating the complex landscape of privacy and data protection laws worldwide. Now in its fourteenth edition, the Handbook has grown to provide an extensive overview of key privacy and data protection regulations across more than 160 jurisdictions. In 2025, the global landscape of data protection and privacy law continues to evolve at an unprecedented pace. With new legislation emerging in jurisdictions around the world, businesses face a growing need to stay informed and agile in adapting to these changes. This year promises to bring new developments and challenges, making the Handbook an invaluable tool for staying ahead in this ever-changing field.

Disclaimer

This handbook is not a substitute for legal advice. Nor does it cover all aspects of the legal regimes surveyed, such as specific sectorial requirements. Enforcement climates and legal requirements in this area continue to evolve. Most fundamentally, knowing high-level principles of law is just one of the components required to shape and to implement a successful global data protection compliance program.

Montenegro

LAST MODIFIED 16 JANUARY 2025

Data protection laws

The Law on Protection of Personal Data, Official Journal of Montenegro, nos. 79/2008, 70/2009, 44/2012 22/2017 and 77/2024, (DP Law) is the governing data protection law. It was first enacted in December 2008 and last amended on 31 July 2024.

The Montenegrin Parliament is expected to adopt a new Data Protection Law to harmonize its data protection law with the EU General Data Protection Regulation (GDPR). However, there is no certainty when exactly, i.e. within which timeframe such adoption (and further implementation) should occur.

Definitions

Definition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable data subject. Data subjects are natural persons whose identity is or can be determined, directly or indirectly, in particular by reference to a personal identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity.

Definition of sensitive personal data

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

- Ethnicity or race
- Political opinion, or religious or philosophical belief
- Trade union membership
- Information on health condition and sexual life

National data protection authority

The Agency for Protection of Personal Data and Free Access to Information (**DPA**) is the local data protection authority. The DPA is currently located at:

Bulevar revolucije 11
Podgorica

Website

www.azlp.me

Registration

Each data controller must do the following:

- Register as a data controller (this registration as a controller is to be performed only once);
- Separately register each database of personal data ('Database') which it intends to establish, before the database is established.

Both registrations must be submitted online through specific forms, whereas the database's registration form is accessible via the DPA's website. The type and scope of the information that must be included in these forms is explicitly prescribed by the DP Law (e.g. the data controller's name and address of its registered seat, name of the Database, legal basis for the processing and purpose of the processing, types of processed data, categories of data subjects, (if applicable) information on any data transfers out of Montenegro). Any significant change to the registered data processing activities, subsequent to the registration should be notified to and registered with the DPA as well.

Exceptionally (i.e. if the intended data processing represents a special risk for the rights and freedoms of individuals), a data controller may, depending on the circumstances of each particular case, be obliged to obtain the DPA's prior approval for such processing (e.g. if biometric data is to be processed without the data subject's consent).

Data protection officers

Under the DP Law, a data controller is required to appoint a DPO subsequent to the Database's establishment. However, a DPO is not required if the data controller has less than ten employees involved in the processing of personal data.

Collection and processing

A prerequisite for the legitimate processing of personal data is to obtain the data subject's valid, informed consent. The consent requirements are explicitly described in the DP Law (e.g. data subjects have to be informed about the purpose and legal basis for the respective processing). The processing of personal data without consent is only allowed under the exceptions listed in the DP Law, (e.g. if the processing is necessary to meet the data controller's statutory obligations under the law or for the protection of life and other vital interests of the data subject who is not capable to personally consent).

As a general matter, in order to comply with the provisions under the DP Law, the processing has to be done in a fair and lawful manner, the type and scope of processed data must be proportionate to the purpose of the respective processing, the data should not be retained longer than necessary in order to meet the defined purpose, and the data has to be accurate, complete and up-to-date.

Transfer of personal data

Under the DP Law, personal data may be transferred to countries or international organizations, where an adequate level of personal data protection exists, subject to the DPA's approval. The DPA issues such approval only where it establishes that adequate measures for the protection of personal data are undertaken (criteria for the adequacy assessment include, for example, the type of the data and the statutory rules in force in the country to which the data is to be transferred).

However, in certain cases the DPA's approval is not required for data transfers out of Montenegro, as explicitly prescribed by the DP Law (e.g. if the data subject consented to the transfer and was made aware of possible consequences of such transfer, or the data is transferred to the European Union or European Economic Area or to any country that the EU Commission has determined ensure adequate level of the data protection).

Security

The DP Law requires that both data controllers and processors undertake technical, personnel and organizational measures for the protection of personal data against loss, destruction, unauthorized access, alteration, publication and misuse. Further, individuals who process personal data are required to keep the processed personal data confidential.

Additionally, data controllers are required to establish internal rules regarding their personal data processing and protection of same (which should include identifying the measures undertaken). Data controllers should also determine which employees have access to the processed data (and to which of this data), as well as the types of data which may be disclosed to other users (and the conditions for the respective disclosure). Finally, if the processing is performed electronically, a data controller is required to ensure that certain information on the use and recipients of the respective data, is automatically kept in the information system.

Breach notification

There is no data security breach notification requirement under the DP Law. However, the Law on Electronic Communications ('Official Journal of Montenegro', nos. 40/2013, 56/2013, 2/2017 and 49/2019) ('EC Law') does impose a duty on operators to, without undue delay, notify the Montenegrin Agency for Electronic Communications and Postal Activity (EC Agency) and the DPA of any breach of personal data or privacy of the data subjects. The affected data subject should also be notified if the breach may have a detrimental effect to their personal data or privacy (unless the EC Agency issues an opinion that such notification is not needed). Failure to comply with any of the above duties is subject to liability and fines, ranging from EUR 6,000 to EUR 30,000 for a legal

entity, and from EUR 300 to EUR 3,000 for a responsible person within a legal entity, and, if some material gain was obtained through the violation, the protective measure, which includes seizure of the respective gain, may be imposed in addition to the above monetary fine.

Enforcement

The DPA is the competent authority for the DP Law's enforcement. It is authorized and obliged to monitor implementation of the DP Law, both ex officio, and upon a third-party complaint.

When monitoring the DP Law's implementation, the DPA is authorized to pass the following decisions:

- Order removal of the existing irregularities within certain period of time;
- Temporarily ban the processing of personal data which is carried out in violation of the DP Law;
- Order deletion of unlawfully collected data;
- Ban transfer of data outside of Montenegro or its disclosure to data recipients carried out in violation of the DP Law;
- Ban data processing by an outsourced data processor if it does not fulfil the data protection requirements or if its engagement as a data processor is carried out in contravention to the DP Law.

The DPA's decisions may not be appealed, but an administrative dispute before the competent court may be initiated against the same.

The DPA may also file a request for the initiation of offence proceeding before a competent Montenegrin court. The offenses and sanctions are explicitly prescribed by the DP Law, which includes monetary fines ranging from €500 to €20,000 for a legal entity and ranging from €150 to €2,000 for a responsible person in a legal entity.

There exists potential criminal liability. The unauthorized collection and use of personal data is a criminal offense under the Montenegrin Criminal Code, punishable with a fine (in an amount to be determined by the court) or imprisonment up to one year (i.e. up to three years if committed by a public official / state servant when performing his duties). Both natural persons and legal entities can be subject to criminal liability.

Electronic marketing

Electronic marketing is not governed by the DP Law. Nevertheless, this law does govern protection of personal data used in direct marketing. In that regard, the law requires that data subjects have to be provided with a possibility to object to the processing of their personal data for direct marketing purposes prior to the commencement of the respective processing. Regarding the use of sensitive personal data in direct marketing, it is explicitly prescribed that a data subject's consent is a requirement for the respective processing.

Although not governed by the DP Law, there are other regulations which govern electronic marketing, including the Law on Electronic Trade ('Official Journal of the Republic of Montenegro', no. 80/04 and 'Official Journal of Montenegro', nos. 41/10, (...), 56/13) ('ET Law'). In this respect, one of the most important rules prescribed by the ET Law is the rule that any sending of unsolicited commercial messages is not allowed unless prior consent of the recipients of the respective marketing is obtained. It is strictly forbidden to send any marketing messages to individuals who have indicated that they do not want to receive such (i.e. opted-out) (and a service provider who sends unsolicited commercial messages is required to establish and maintain a record of individuals who opted-out). A violation of the respective rules is subject to liability, with fines ranging from EUR 500 to EUR 17,000 (for a legal entity) and ranging from EUR 100 to EUR 1,500 (for a responsible person in a legal entity). For particularly serious violations or repeated violations, an order banning or suspending the business activity (lasting from three months to six months) may be imposed on an entity responsible for the respective violations).

Online privacy

There is no specific law or regulation explicitly governing online privacy, including cookies. Accordingly, the general data protection rules, as introduced by the DP Law, are applicable to online privacy, to the extent personal data is processed.

On the other hand, the EC Law, as defined in Breach notification, introduces relevant rules that are mandatory for the operators under this law. For example, a public electronic communication services' user is particularly entitled to the protection of their electronic communications' secrecy in compliance with the DP Law.

Further, the EC Law imposes explicit rules on traffic data and location data. Under these rules, operators are:

- Required to retain certain traffic data and location data for certain purposes explicitly set out by the law (for example, for the detection and criminal prosecution of criminal offenders), whereas the retention period should last at least six months and would not be longer than two years ('Retention Obligation'), keeping in mind that this obligation does not apply to data which reveals a content of electronic communications.
- Regarding traffic data related to subscribers / users which is not subject to the Retention Obligation, an operator is required to delete this data if it is no longer needed for the communication's transmission or can keep it, but only if it modifies the respective data in a way that it cannot be linked to a particular person. Apart from this, it is also prescribed that:
    - If the traffic data's retention purpose is to use it for the calculation of the costs of the relevant services / interconnection, it can be retained for as long as claims regarding the respective costs can legally be requested, but under condition that an user is informed on its processing's purpose and duration; and that

- If the traffic data's processing purpose is to promote and sell electronic communication services or to provide value added services, such processing is allowed, but only with the data subjects' prior consent (which can be withdrawn at any time).

- Regarding location data which is not subject to the Retention Obligation, an operator is allowed to process it but only with the data subject's consent (which can be withdrawn at any time) or if the respective data is modified in a way that it cannot be linked to a particular person without consent.

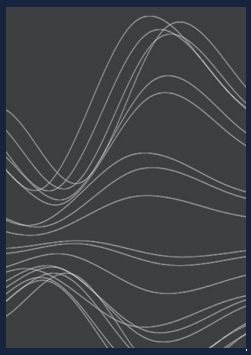
Failure to comply with any of the above rules regarding the processing of traffic or location data which is not covered by the above-identified Retention Obligation, is subject to offence liability and fines in range from EUR 4,000 to EUR 20,000 for a legal entity, and in range from EUR 200 to EUR 2,000 for a responsible person in a legal entity.

Data protection lawyers

Sanja Spasenović
Attorney at Law
Karanovic & Partners
sanja.spasenovic
@karanovicpartners.com
View bio

For more information

To learn more about DLA Piper, visit dlapiper.com or contact:



Carolyn Bigg
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
carolyn.bigg@dlapiper.com
Full bio

John Magee
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
john.magee@dlapiper.com
Full bio

Andrew Serwin
Partner
Global Co-Chair Data, Privacy and Cybersecurity Group
andrew.serwin@us.dlapiper.com
Full bio

About us

DLA Piper is a global law firm with lawyers located in more than 40 countries throughout the Americas, Europe, the Middle East, Africa and Asia Pacific, positioning us to help companies with their legal needs around the world.

dlapiper.com

This publication is for general information only. The information presented is not legal advice, and your use of it does not create a lawyer-client relationship. All legal matters are unique and any prior results described in this publication do not guarantee a similar outcome in future matters. DLA Piper is a global law firm operating through DLA Piper LLP (US) and affiliated entities. For further information, please refer to dlapiper.com. Attorney Advertising. Copyright © 2025 DLA Piper LLP (US). All rights reserved.