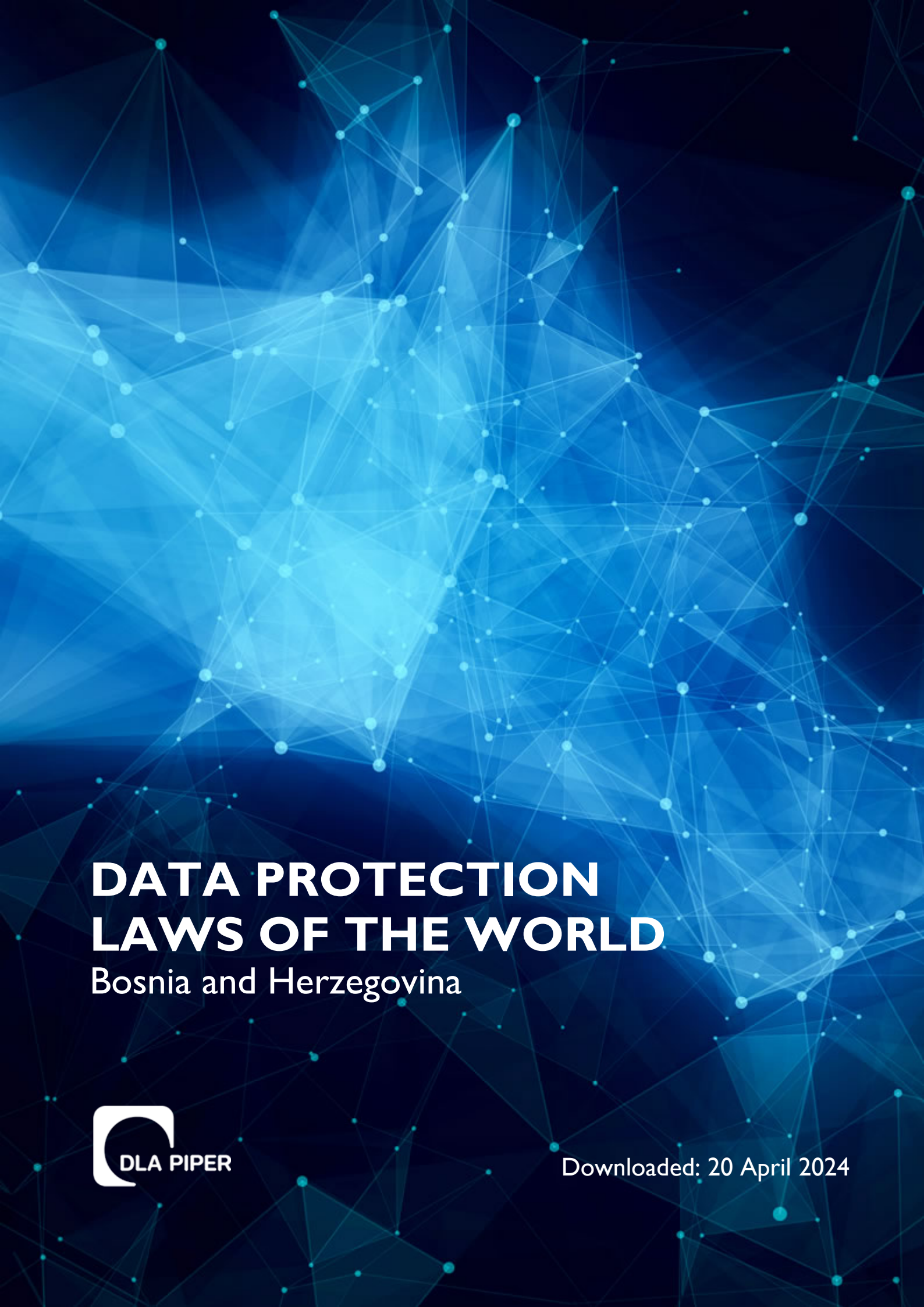
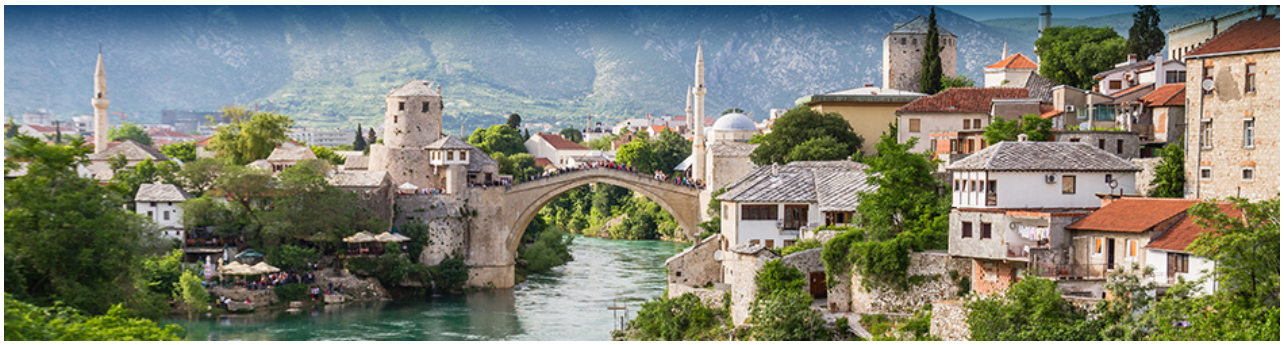


# DATA PROTECTION LAWS OF THE WORLD

## Bosnia and Herzegovina

DLA PIPER

# BOSNIA AND HERZEGOVINA



*Last modified 21 December 2022*

## LAW

The Law on Protection of Personal Data ('Official Gazette of BIH', nos. 49/06, 76/11 and 89/11) (DP Law) is the governing law regulating data protection issues in Bosnia and Herzegovina (BiH). The DP Law came into force on July 4, 2006 and was amended on October 3, 2011.

Due to the deficiencies and non-alignment of the DP Law with the GDPR, in 2018, the competent authorities initiated the procedure for adoption of a new GDPR compliant data protection law in BiH. According to the publicly available information the draft of the new data protection law (Draft Data Protection Law), was forwarded to the BiH Ministry of Civil Affairs and the adoption procedure before the BiH Parliament should have been initiated. However, due to the complex political the Draft Data Protection Law is not adopted to date. However, we expect the Draft Data Protection Law to be adopted in its current text within the following year.

## DEFINITIONS

### Definition of personal data

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

### Definition of sensitive personal data

The DP Law defines sensitive personal data as any data relating to any of the following:

- Racial, national or ethnic origin;
- Political opinion, party affiliation, or trade union affiliation;
- Religious, philosophical or other belief;
- Health;
- Genetic code;
- Sexual life;
- Criminal convictions; and
- Biometric data.

Definitions of sensitive personal data stipulated by Draft Data Protection Law correspond to the definitions prescribed by GDPR.

## NATIONAL DATA PROTECTION AUTHORITY

The Personal Data Protection Agency (DPA) is the national data protection authority in BiH. The DPA is seated in:

*Dubrovačka 6*
*Sarajevo*
www.azlp.ba

The DPA remains national data protection authority under Draft Data Protection Law.

## REGISTRATION

Each data controller (defined as a person or legal entity which processes personal data) must provide the DPA with specific information on the database containing personal data ("**Database**") established and maintained by the controller. The DPA maintains a publicly available register of data controllers and Databases.

The Database's registration includes two phases:

- First, the controller must register as a data controller (this registration as a controller is to be performed only once).
- Second, the controller must report to the Database's establishment, which has to be done within 14 days.

Registration of the Database is made by submitting the application in the prescribed form to the DPA. The DPA form includes information regarding:

- Data controller
  - Name
  - Address of its registered seat
- The Database itself
  - Processing purpose
  - Legal ground for its establishment
  - Identification of exact processing activities
  - Types of processed data
  - Categories of data subjects, and
  - Transfer of data abroad

If there is a subsequent change in the registered data, for example changing initial processing activities, the change needs to be reported to the DPA within 14 days from the date the change occurred.

Unlike the DP Law, the Draft Data Protection Law foresees the obligation of data controllers and data processors to keep records of their data processing activities identically as the GDPR, however it does not oblige data controllers to register their data processing activities/databases with the Agency.

## DATA PROTECTION OFFICERS

There is no statutory obligation that the entity which processes personal data has a data protection officer. The Rules on the Manner of Keeping and Special Measures of Personal Data Technical Protection (Official Gazette of BiH no. 67/09) (Rules) stipulate that a controller can have an administrator of the Database. Such administrator is a natural person authorized and responsible for managing the Database and ensuring privacy and protection of personal data processing, in particular regarding implementation of security measures, storage and protection of data.

Unlike DP Law, the Draft Data Protection foresees the obligation of data controller and processor to ensure properly and timely involvement of the data protection officer in all issues related to the protection of personal data. Position and tasks of data protection officer envisaged by Draft Data Protection Law correspond to those prescribed by GDPR.

## COLLECTION & PROCESSING

Collection and processing of personal data is permissible if carried out pursuant to the data subject’s consent and in compliance with the basic principles of personal data protection.

The form of the data subject’s consent depends on the type of personal data collected and processed. While the collection and processing of sensitive personal data requires explicit written consent from the data subject, the consent for the collection and processing of personal data falling within a category of general personal data does not have to be in writing. However, at the request of the competent authority, the controller has to be able to prove, at any time, the existence of a data subject’s consent for processing of both personal and sensitive personal data. Therefore, having a written consent for collection of any personal data is advisable. When required, written consent must contain at minimum elements prescribed by the DP law.

Apart from the consent, there are also other conditions which must be met for the collection and processing to be regarded as legitimate, including:

- Processing must be done in a fair and lawful way;
- The type and scope of processed data must be proportionate to the respective purpose; and
- Other principles regarding the legitimate reasons for personal data processing.

The DP Law provides an exception when a data subject's personal data may be processed without the data subject’s consent. This is the case where the processing is necessary for the fulfillment of a data controller’s statutory obligations or for preparation or realization of an agreement concluded between a data controller and a data subject (Exceptional Cases). These conditions are considered the basic principles of personal data protection and are applicable to each case of personal data processing.

The legal grounds as well as the data processing requirements envisaged by the Draft Data Protection Law fully correspond to those envisaged by the GDPR.

## TRANSFER

Under the transfer rules set out in the DP Law, processed personal data may be transferred to countries where an adequate level of personal data protection is ensured. In that regard, preferential status is given to the member states of the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ("**Convention**"), as members of the Convention ensure an adequate level of personal data protection.

Personal data transfer to countries that do not provide for an adequate level of personal data protection is allowed in certain cases stipulated by the DP Law, for example:

- When the data subject consented to the transfer and was made aware of possible consequences of such transfer;
- When it is required for the purpose of fulfilling the contract or legal claim; or
- When it is required for the protection of public interest.

In addition, the DPA may exceptionally approve the transfer to a country that does not ensure adequate an level of personal data protection if the controller in the country where the data is to be transferred can provide for sufficient guarantees in regard to the protection of privacy and fundamental rights and freedoms of the data subject.

The Draft Data Protection Law prescribes a set of mechanisms based on which a legitimate transfer of data out of BiH is possible. This means that the Draft Data Protection Law tends, the same as the GDPR, to enable legitimate transfer of personal data whenever there are some safeguards that transferred data will be processed in line with the law.

Aforementioned means the following:

- It should firstly be checked whether a particular country to which the data is to be transferred is regarded as a country with an adequate data protection system (“**Adequate Country**”);
- If a country to which the data is to be transferred from BiH is the Adequate Country or if there is a data transfer related international treaty entered into between BiH and that country, a transfer is possible without any approval of the Agency (“**Transfer Approval**”);
- On the other hand, if a country to which the data is to be transferred is not the Adequate Country, a transfer is still possible without the Transfer Approval if the adequate data protection measures are undertaken (e.g., if appropriate standard contractual clauses have been entered into between a data exporter and a data importer) (“**Adequate**

**Safeguards**”);

- However, even if there are no Adequate Safeguards, there is still a possibility for transferring the data without the Transfer Approval. Such possibility exists in so-called special situations, explicitly prescribed by the Draft Data Protection Law, the same as under the GDPR (e.g., a data subject has consented to a particular transfer, a transfer is necessary for the realization of an agreement between a data subject and data controller, etc.);
- Finally, even if none of the aforementioned special situations is applicable, a data transfer is still allowed without the Transfer Approval if certain conditions (linked to a data controller's legitimate interest) explicitly prescribed by the Draft Data Protection Law are cumulatively fulfilled.

## SECURITY

The DP Law requires data controllers and processors to:

- Take care of data security and to undertake all technical and organizational measures;
- Undertake measures against unauthorized or accidental access to personal data, their alteration, destruction or loss, unauthorized transfer, other forms of illegal data processing, as well as measures against misuse of personal data; and
- Adopt a personal data security plan ("**Security Plan**") which specifies technical and organizational measures for the security of personal data.

As provided by the Rules (as defined in the section "**Data Protection Officers**"), the Security Plan includes the categories of processed data and the list of instruments for protection of the data to ensure confidentiality, integrity, availability, authenticity, possibility of revision and transparency of the personal data.

The Rules prescribe that the controller is required to undertake more stringent technical and organizational measures when processing sensitive personal data. Such measures aim at enabling recognition of each authorized access to the information system, operation with the data during the controller’s regular working hours and cryptographic protection of the data transmission via telecommunications systems with appropriate software and technical measures.

The Rules also closely regulate the manner of personal data keeping and personal data protection in automatic processing.

Security measures envisaged by Draft Data Protection Law correspond to the measures prescribed by GDPR.

## BREACH NOTIFICATION

The DP Law does not impose data security breach notification duty on the controller. However, the Rules do impose a duty on the Database's administrator, processor and performer to inform the controller on any attempt of unauthorized access to information system for the Database's management.

However, the regulations issued by the Communication Regulatory Agency (RAK) should be considered. The Regulation on Carrying out the Activities of the Publicly Available Electronic Communication Networks ('Official Gazette of BiH' no. 66/12) (Regulation A) stipulates that the operator of publicly available electronic communication networks (Operator) is required to inform RAK about its activities, operations and other applicable information required for RAK’s regulatory competences. Since RAK’s Regulation on Conditions for Providing the Telecommunications Services and Relation with End Users ('Official Gazette of BiH' no. 28/13) (Regulation B) prescribes for the Operator’s obligation to undertake such methods which will protect the privacy of users and others, in a manner that will ensure the integrity and confidentiality of data, it can be concluded that the Operator is required to notify RAK of any breach of security and integrity of public telecommunication services that resulted in violation of protection of personal data or privacy of the respective services' s users.

When it comes to the notification duty towards the users, the Regulation B obliges the Operator to inform the users adequately (e.g. in user agreement, in its terms and conditions or in the appropriate technical way) about the possibility of privacy or telecommunication facilities violations.

Pursuant to the Draft Data Protection Law in case of a personal data breach the controller is obliged to undue delay and where feasible not later than 72 hours after having become aware of it, which fully correspond to the obligation prescribed by GDPR.

## ENFORCEMENT

The DPA enforces the DP Law. The DPA is authorized and obliged to monitor implementation of the DP Law, both *ex officio*, and upon a third-party complaint. If the DPA finds that a particular person or entity processing personal data acted in violation of data processing rules, it may request that the controller discontinue such processing and order specific measures to be carried out without delay.

When acting upon the complaints, the DPA may also issue a decision by which it can order blocking, erasing or destroying of data, adjustment or amendment of data, temporary or permanent ban of processing, issue warning or reprimand to the controller. The decision of the DPA may not be appealed; however, a party may initiate administrative dispute before the Court of BiH.

The DPA can initiate a misdemeanor proceeding against the respective data controller before the competent court, depending on the gravity of the particular misconduct and the data controller’s behavior with respect to the same. The offenses and sanctions are explicitly prescribed by the DP Law, which includes monetary fines for a controller in the amount between €2,550 and €51,100, as well as for the controller's authorized representative in the amount between €100 and €7,700.

The Draft Data Protection Law, although still not as strict as the GDPR, foresees fines which are significantly higher than the ones foreseen by the Current Data Protection Law. Specifically, the Draft Data Protection Law introduces fines in the amount of up to BAM 200,000 (approx. EUR 100,000) or 4% of the total worldwide annual turnover of the preceding financial year (whichever is higher).

Breach of personal data protection regulations represents a criminal offense of unauthorized collection of personal data by all criminal codes applicable in BiH (Criminal Code of BiH, Criminal Code of the Republic of *Srpska*, Criminal Code of the Federation of BiH and Crimes Code of *Brčko Distrikt*). Prescribed sanctions are monetary fines (in amount to be determined by the court) or imprisonment up to six (6) months (Criminal Code of BiH; Criminal Code of the Federation of BiH; Criminal Code of the *Brčko Distrikt*) or up to one (1) year (Criminal Code of the Republika *Srpska*).

## ELECTRONIC MARKETING

Although electronic marketing is not governed by the DP Law, the respective law regulates protection of personal data used in direct marketing. In that regard, the controller is not allowed to disclose personal data to a third party without the data subject’s consent. However, when that is necessary for the protection of the controller’s rights and interests and when it is not in contradiction with the data subject’s right to the protection of personal privacy and personal life, the personal data may be used for direct marketing purposes without consent. The DPA is of the opinion that previous provision could be used only in explicit cases, when the controller is offering products or services to regular client in order to limit possible future damages for which he could be held responsible.

Under Regulation B, the Operator is prohibited from using user personal data for purposes of its business or other promotions, unless it obtains explicit consent from the user to whom such data relates.

## ONLINE PRIVACY

The general data protection rules, as introduced by the DP Law, are relevant for online privacy as well, as there are no specific regulations that explicitly govern online privacy. This includes obligation to act in accordance with the basic principles of personal data protection set out in the DP Law as well as acting on the basis of the data subject's informative consent.

## KEY CONTACTS

**Karanovic & Nikolic**
www.karanovic-nikolic.com/

Nihad Sijercic
Attorney-at-law in cooperation with Karanovic & Partners
T +387 33 844 000
nihad.sijercic@karanovicpartners.com

Amina Dugum
Attorney-at-law in cooperation with Karanovic & Partners
T +387 33 844 000
amina.djugum@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.