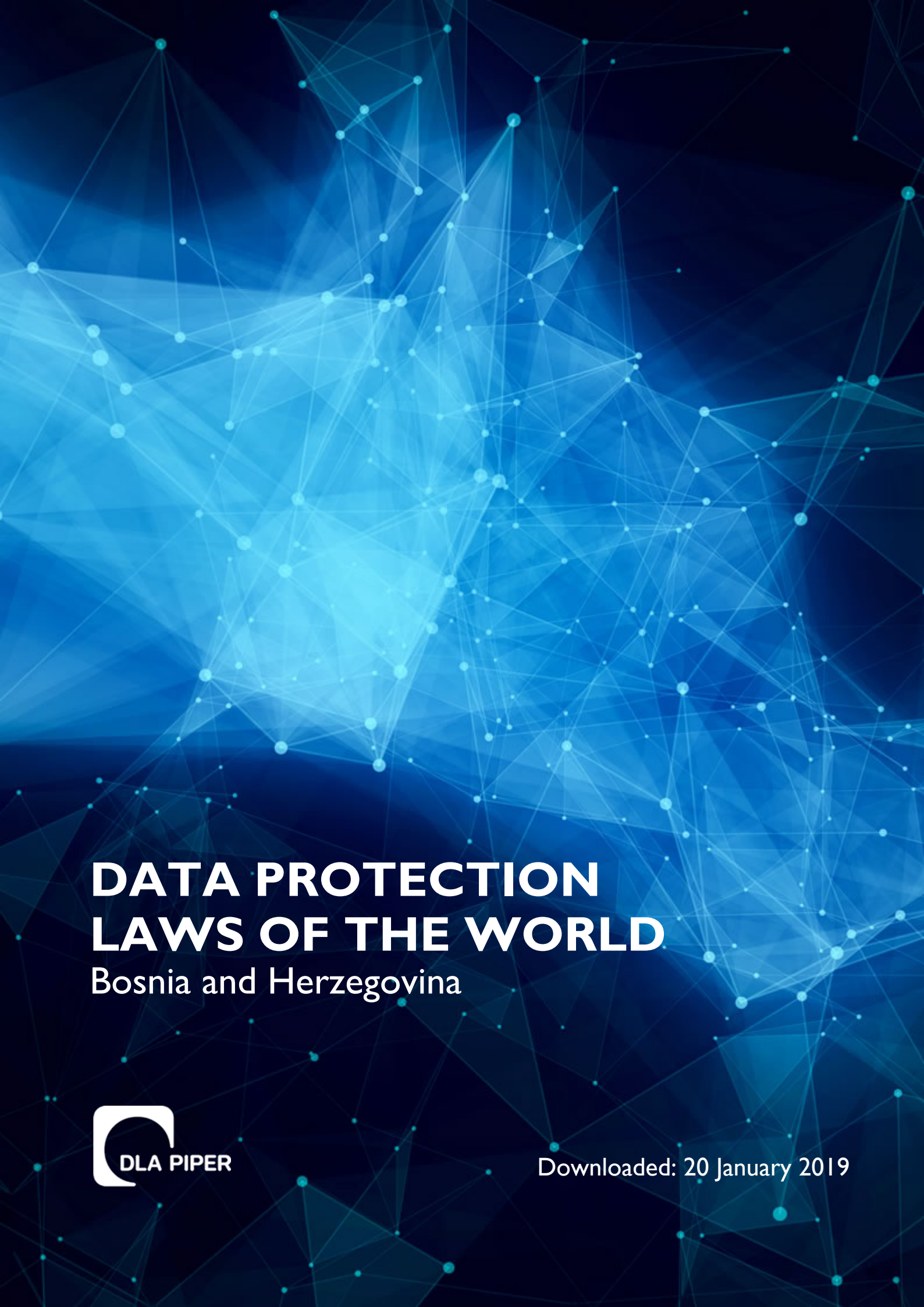
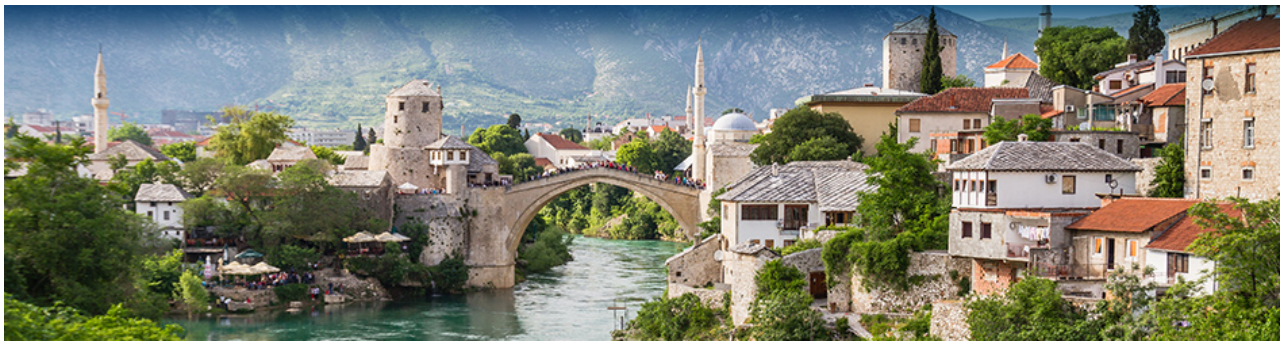


DATA PROTECTION LAWS OF THE WORLD

Bosnia and Herzegovina

DLA PIPER

BOSNIA AND HERZEGOVINA



Last modified 25 January 2017

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 entered into force on 4 July 2006 and its current version (after amendments made in 2011) is in force from 3 October 2011.

DEFINITIONS

Defenition of personal data

The DP Law defines personal data as any information relating to an identified or identifiable natural person. The 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/her physical, physiological, mental, economic, cultural or social identity.

Defenition of sensitive personal data

The DP Law defines sensitive personal data as any data relating to

- 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.

NATIONAL DATA PROTECTION AUTHORITY

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

Vilsonovo šetalište 10
Sarajevo
www.azlp.gov.ba

REGISTRATION

Each data controller (defined as a person or legal entity which processes personal data) has to provide the DPA with specific information on the database containing personal data ('Database') established and maintained by the controller. The DPA keeps

publicly available register of data controllers and Databases.

The Database's registration includes two phases:

1. the first phase represents notification of intention to establish the Database to the DPA
2. the second phase includes reporting 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
  - its name, and
  - address of its registered seat, and
- 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 etc.

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.

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.

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 needed, written consent has to contain 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 legitimate. These conditions are considered the basic principles of personal data protection and are applicable to each case of personal data processing. For example, 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 which guarantee legitimate reasons for personal data processing.

The DP Law provides for the 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 fulfilment 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').

TRANSFER

Under the transfer rules set out in the DP Law, processed personal data may be transferred to countries where 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'), since it is considered that countries – members of the Convention ensure adequate level of personal data protection.

Personal data transfer to countries which do not provide for 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 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.

SECURITY

The DP Law prescribes that both data controllers and, within the scope of their competencies, the processors are required:

- to take care of data security and to undertake all technical and organizational measures
- to 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
- to adopt 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.

Moreover, 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.

Manner of personal data keeping and personal data protection in automatic processing is also closely regulated by the Rules.

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 (eg in user agreement, in its terms and conditions or in the appropriate technical way) about the possibility of privacy or telecommunication facilities violations.

ENFORCEMENT

Enforcement of the DP Law is done by the DPA. 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/entity processing personal data acted contrary to the data processing rules, it may request from the controller to 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 misdemeanour proceeding against the respective data controller before the competent court, depending on the gravity of the particular misconduct and the data controller's behaviour with respect to the same. The offences and sanctions are explicitly prescribed by the DP Law, which includes monetary fines for a controller in the amount between approximately EUR 2,550 and EUR 51,100, as well as for the controller's authorized representative in the amount between approx. EUR 100 and EUR 7,700.

Breach of personal data protection regulations represents a criminal offence 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 *Brko 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 *Brko Distrikt)* or up to one (1) year (Criminal Code of the Republic of *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 the Regulation B, the Operator is not allowed to use personal data of the users for the purposes of its business or other promotions, unless it obtained explicit consent from the users to whom such data relates.

ONLINE PRIVACY

The general data protection rules, as introduced by the DP Law, are relevant for on-line privacy as well, as there are no specific regulations that explicitly govern on-line 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/

Mirna Milanovi Lalic
Senior Associate
T +387 33 261 535
mirna.lalic@karanovic-nikolic.com

Lana Deljkic
Senior Associate
T +387 33 261 535
lana.deljkic@karanovic-nikolic.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organisation'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.