



INTERNATIONAL
LAWYERS
NETWORK

2024

ILN DATA PRIVACY GUIDE

An International Guide

www.iln.com



ILN Cybersecurity & Data Privacy Group and ILN
Technology Media & Telecommunications Group



Disclaimer

This guide offers an overview of legal aspects of data protection in the requisite jurisdictions. It is meant as an introduction to these marketplaces and does not offer specific legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship, or its equivalent in the requisite jurisdiction.

Neither the International Lawyers Network or its employees, nor any of the contributing law firms or their partners or employees accepts any liability for anything contained in this guide or to any reader who relies on its content. Before concrete actions or decisions are taken, the reader should seek specific legal advice. The contributing member firms of the International Lawyers Network can advise in relation to questions regarding this guide in their respective jurisdictions and look forward to assisting. Please do not, however, share any confidential information with a member firm without first contacting that firm.

This guide describes the law in force in the requisite jurisdictions at the dates of preparation. This may have been some time ago and the reader should bear in mind that statutes, regulations, and rules are subject to change. No duty to update information is assumed by the ILN, its member firms, or the authors of this guide.

The information in this guide may be considered legal advertising.

Each contributing law firm is the owner of the copyright in its contribution. All rights reserved.

About the ILN

The ILN is a non-exclusive network of high-quality mid-sized law firms, which operates to create a global platform for the provision of legal services, particularly for clients with international needs. With a presence in 67 countries, it is exceptionally well placed to offer seamless legal services, often of a cross-border nature from like-minded and quality legal practices. In 2021, the ILN was

honored as Global Law Firm Network of the Year by The Lawyer European Awards, and in 2016, 2017, 2022, and 2023 they were shortlisted as Global Law Firm Network of the Year. Since 2011, the Network has been listed as a Chambers & Partners Leading Law Firm Network, increasing this ranking in 2021 to be included in the top two percent of law firm networks globally. Today, the ILN remains at the very forefront of legal networks in its reach, capability, and depth of expertise.

Authors of this guide:

1. **Cybersecurity & Data Privacy Group**

Co-chaired by Jim Giszczak of McDonald Hopkins and Stuart Gerson of Epstein Becker & Green, the Cybersecurity & Data Privacy Specialty Group provides an international platform for enhanced communication, enabling all of its members to easily service the needs of their clients requiring advice.

2. **Technology, Media & Telecom (TMT)**

Co-chaired by Alishan Naqvee of LexCounsel in New Delhi and Gaurav Bhalla of Ahlawat & Associates in New Delhi the TMT Group provides a platform for communication on current legal issues, best practices, and trends in technology, media & telecom.



Czech Republic

Introduction

The General Data Protection Regulation (Regulation (EU) 2016/679) is the EU regulation which is directly applicable in all member states of the EU, including the Czech Republic, as of 25 May 2018. The new Czech Act No. 110/2019 Coll., on Processing of Personal Data, which partly implements the GDPR in the Czech Republic, is effective as of 24 April 2019. The Act on Processing of Personal Data replaced the previous Act No. 101/2000 Coll., on Protection of Personal Data, as amended. Among other things, this new act regulates jurisdiction of the Office for Personal Data Protection as the main data protection authority in the Czech Republic. The other laws briefly described below contain special rules for specific areas which apply together with or beside the general rules on personal data protection and processing.

Contact Us

☎ +420 246 085 300

🌐 www.peterkapartners.com/

✉ hradil@peterkapartners.cz

📍 Karlovo náměstí 671/24
110 00 Praha 1

Governing Data Protection Legislation

2.1 Overview of principal legislation

- the Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) ("GDPR");
- the Act no. 110/2019 Coll., on the Processing of Personal Data, as amended (this act implements the GDPR in the Czech Republic).

2.2 Additional or ancillary regulation, directives or norms

- the Act No. 89/2012 Coll., Civil Code, as amended (with general rules on privacy in section 84 and following);
- the Act No. 262/2006 Coll., Labour Code, as amended (it stipulates some rules on privacy in employment, namely in section 316 of the Labour Code);

Czech Republic

- the Act No. 480/2004 Coll., on Certain Information Society Services and on Amendments to Certain Acts, as amended (“Act on Certain Information Society Services”) (the dissemination of commercial communications by electronic means, such as by e-mail or telephone, is regulated by this act). This act implements the Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (“Directive on electronic commerce”) and the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (“ePrivacy Directive” or “ePD”);
- the Act No. 127/2005 Coll., on Electronic Communications and on Amendment to Certain Related Acts (Act on Electronic Communications), as amended (this act regulates the marketing phone calls, use of cookies and processing of personal data in telecommunications). This act implements, among others, the Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code, and also the ePrivacy Directive/ePD;
- the Act No. 181/2014 Coll., on Cyber Security, as amended
 - (with several obligations, for example the registration obligation and the obligation to report security incidents under the Cyber Security Act in addition to obligation to report data breaches under the GDPR/eDP – in case the data breach involves also security incident).

2.3 Upcoming or proposed legislation (if applicable)

- the new act on cyber security replacing the Cyber Security Act mentioned above should be adopted and effective as of October 2024 in the Czech Republic. This new act is implementing the Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

Scope of Application

3.1. Legislative Scope

The general rules for the protection and processing of personal data in the Czech Republic are stipulated in Act No. 110/2019 Coll., on the Processing of Personal Data, as amended (“Act on Processing of Personal Data”), and Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC – (General Data Protection Regulation) (“GDPR”).

3.1.1. Definition of personal data

The same as in the GDPR.

3.1.2. Definition of different categories of personal data

There are no special definitions of other personal data, except for regulation of birth number, which is a unique identifier (identification number) of natural persons in the Czech Republic (similar to social security number in other countries). There are other terms such as “sensitive data” or “sensitive personal

data” used in previous law and legal regulations (where these previous laws and/or regulation use the terms above, this basically means special categories of personal data under the GDPR – see also point 3.2 below).

3.1.3. Treatment of data and its different categories

-Regulation of personal and non-personal data

The personal data and their processing are regulated namely by the GDPR and the Act on Processing of Personal Data. As for non-personal data, the safety of selected networks and provision of relevant services by selected obliged persons is regulated namely by the Cyber Security Act.



-Regulation of electronic and non-electronic data

There is no special regulation distinguishing the data based on the form of data (electronic or non-electronic), the regulation of personal data applies to all data disregarding their form, with very few exceptions (such as special regulation for direct marketing via e-mail or phone calls, which is regulated mainly by the Act on Certain Information Society Services and the Act on Electronic Communications).

3.14. Other key definitions pertaining to data and its processing

The definitions are the same as in the GDPR, the Act on Personal Data Processing does not contain any different or special definitions related to personal data and their processing.

3.2. Statutory exemptions

There are only few exemptions or special requirements under the Czech law in addition to the GDPR. The most important ones are briefly described below:

- The implementation of article 6.2 of GDPR: Article 6.2 of GDPR has only been partially addressed in the Act on Processing of Personal Data, namely in Title II, Personal Data Processing Pursuant to Directly Applicable Regulation of the European Union (i.e., GDPR), Chapter 1 (namely sections 5, 6, 8, 9, 10, 11, 12 and 14). Chapter 2 deals with Personal Data Processing for Journalistic Purposes or Purposes of Academic, Artistic or Literary Expression.

- The implementation of article 8.1. of GDPR: Under section 7 of the Act on Personal Data Processing, there is a fifteen years of age limit for a child to grant consent to personal data processing in relation to an offer of information society services addressed directly to the child (for more details see point 7 below).
- The implementation of Article 9.4 of GDPR: Article 9.4 of GDPR has not been expressly addressed in the Act on Processing of Personal Data implementing the GDPR in the Czech Republic, it only mentions these data (genetic, biometric data or of data



- concerning health) in section 66 (Transitory Provisions), together with other data referred to as “sensitive data” or „sensitive personal data“ in previous law and legal regulations (where these previous laws and/or regulation use the terms above, this basically means special categories of personal data under the GDPR).
- The implementation of Article 23.1 of GDPR: Article 23.1 of GDPR has been addressed in the Act on Processing of Personal Data implementing the GDPR in the Czech Republic, namely in Title II, Personal Data Processing Pursuant to Directly Applicable Regulation of the European Union, and Title IV, Personal Data Protection in Ensuring Defence and Security Interests of the Czech Republic.
- The implementation of Article 35.4 of GDPR: In the implementation of Article 35.4 of GDPR, the Office has issued the lists and the methodologies related to DPIA (the Office published not only the list of activities under the article 35(4) of the GDPR, but also the list of activities under the article 35(5) of the GDPR).
- The implementation of Article 35.10 of GDPR: Under section 10 of the Act on Personal Data Processing, the controller does not have to carry out an assessment of the impact of the processing on the protection of personal data (DPIA) before it begins, if the legal regulation requires him to carry out such processing of personal data.
- The implementation of article 87 of GDPR: The regulation of the use of the birth (identification) number is contained in the Act No. 133/2000 Coll., on the Registration of Population and Birth Numbers and on the Amendment of Certain Acts (the Act on Population Registration). Pursuant to Section 13(9) of this act, only the natural person to whom the birth number has been assigned (or his / her legal representative) is entitled to use it or decide on its use within the limits stipulated by law; otherwise, the birth number may be used only in the cases specified in Section 13c of this act.
- The implementation of Article 88 of GDPR: The implementation of Article 88 of GDPR, which deals with processing in the context of employment, has been dealt with namely in section 316 of the Labour Code.

3.3 Territorial and extra-territorial application

In general, the laws of the Czech Republic apply within the territory of the Czech Republic. As for the GDPR, the provisions of article 3 apply, including extraterritorial application of the GDPR.

Legislative Framework

4.1 Key stakeholders

- There are no derivations based on the local law from the definitions in the GDPR, i.e., the

definition for each stakeholder such as 'Data Controller', 'Data Processor', 'Data Subject' etc., are the same as under the GDPR.

4.2 Role and responsibilities of key stakeholders

All key stakeholders must be able to prove that they fulfil all requirements stipulated by personal data protection laws, including the Czech local law and the GDPR. As for the language, the Office may require Czech translations or Czech versions of the Czech companies' (as data controllers or data processors) documents on personal data processing/protection. Under the Czech law, there is no express provision regarding the language in which such internal guidelines/policies/documentation should be drafted. However, in the field of data protection the activity carried out by a controller/processor is subject to the investigation by Czech authorities, namely the Office, based on the Czech law. In this respect, the Czech authorities may require either bilingual documents or certified translations into Czech language of documents issued in a different language. Thus, at least a bilingual version including Czech version or a certified translation into Czech should be available for the relevant authorities.

Requirements for Data Processing

5.1 Grounds for collection and processing

- Consent: No derivations from the GDPR.

- Consent Notice: No derivations from the GDPR.
- Withdrawal of Consent: No derivations from the GDPR.

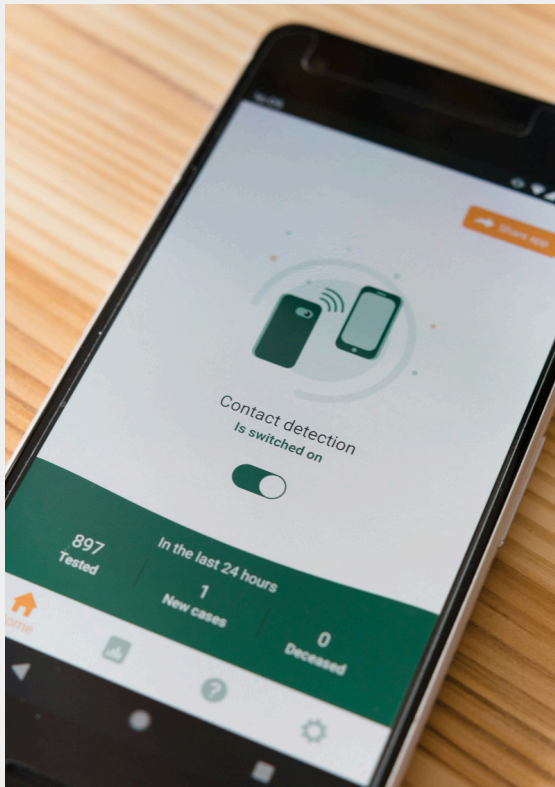
5.2 Data storage and retention timelines

There are no explicit general rules stipulating data retention periods, only some special laws mention such periods. For example, personal data that need to be processed for accounting purposes must be, generally, kept for 5 years as of the end of accounting period for all accounting documents if not stipulated otherwise (under the Accounting Act), 10 years for financial statements and annual reports (under the Accounting Act), for VAT purposes (under the Value Added Tax Act) and for social security payments purposes (under the Act on Social Security Contributions and Contribution to the State Employment Policy) or generally for tax purposes (under the Act on Income Taxes and the Tax Code) and 30 years for pensions purposes must be kept up to (under the Act on the Organization and Implementation of Social Security). If the personal data are needed for debt collection they must be kept until the end of the first financial year following the financial year in which the debt was paid or obligation met (under the Accounting Act).

Where accounting units use accounting records not only for the purpose pursuant to the Accounting Act, but also for other purposes, in particular for purposes relating to

Czech Republic

criminal proceedings, measures against money-laundering (keeping the records for 10 years), administrative proceedings, civil judicial proceedings, tax proceedings or special proceedings concerning the destruction of certain documents or for the purposes of social security, general health insurance or copyright protection, after expiry of the storing periods above, the accounting units are obliged so proceed as to ensure compliance with the requirements ensuing from the use of accounting records for such other purposes; in cases in which the accounting units use their accounting records for such purposes, all the provisions of the Accounting Act similarly apply.



As for the CCTV recordings, based on the opinions of the Office, the standard retention period recordings from the CCTV, is 3 to 7 days in the Czech Republic. Any longer retention period must be justified by circumstances of the particular case (unless there are special rules stating otherwise, such as regulations for gambling).

As for the traffic and location data, the data retention is regulated in the Czech Republic by the Act on Electronic Communications. Under Sec. 97(3) of the Act on Electronic Communications, a legal entity providing a public communications network or a publicly available electronic communications service is obliged to store traffic and location data for a period of 6 months and is obliged to disclose such data (including metadata) to the relevant authorities (e.g., police) on request (please note that this applies only to providers of services under the Act on Electronic Communications).

5.3. Data correction, completion, updation or erasure of data

No derivations from the GDPR.

5.4. Data protection and security practices and procedures

No derivations from the GDPR. The Office publishes guidelines of the EDPB and also its own guidelines regarding selected security practices and procedures in personal data protection area.



5.5. Disclosure, sharing and transfer of data

No derivations from the GDPR.

5.6. Cross border transfer of data

No derivations from the GDPR.

5.7. Grievance redressal

No derivations from the GDPR. In most cases, the Czech Office for Personal Data Protection is the local DPA (data protection authority) who deals with complaints.

Rights and Duties of Data Providers/Principals

6.1 Rights and remedies

- Right to withdraw consent: No derivations from the GDPR, if the processing is based on consent, the consent may be withdrawn anytime.

- Right to grievance redressal and appeal: The Czech Office for Personal Data Protection (Office) is the local DPA (data protection authority) who deals with complaints. It is possible to file an appeal against the decision of the Office to the Chairperson of the Office. It is possible to file an administrative action in the Municipal Court in Prague against the final decision of the Office.
- Right to access information: No derivations from the GDPR.
- Right to nominate: There is no explicit regulation of the right to nominate in the Czech law regarding processing of personal data. Primarily, it is the data controller who is responsible for data processing activities and

performing related duties. Personal data controller may appoint personal data processor(s) to perform some of these data processing activities.

6.2 Duties

As for the data processing, the duties of data controllers and data processors are the same as under the GDPR. For the main roles and responsibilities of key stakeholders, including language requirements, please see above point 4.2. For the main

Processing of Children or Minors' data

As regards the consent of minors for the data processing, referred to in Article 8.1 of GDPR, this provision has been implemented by section 7 of the Act on Personal Data Processing (Capacity of Child to Grant Consent to Personal Data Processing), under which "A child shall enjoy capacity to grant consent to personal data processing in relation to an offer of information society services addressed directly to the child from fifteen years of age".

Regulatory Authorities

8.1 Overview of relevant statutory authorities

- The Czech Office for Personal Data Protection (ÚOOÚ)
- The Czech Telecommunication Office (ČTÚ)
- The National Cyber and Information Security Agency (NÚKIB) and CZ.NIC

8.2 Role, functions and powers of authorities

- Role functions and powers of principal data regulation authority (if applicable): In the Czech Republic, the Office for Personal Data Protection (hereinafter "Office") supervises observance of the legal obligations laid down for the processing of personal data as the main authority in this area. Supervision in the form of inspection is performed pursuant to a special act (Act no. 255/2012 Coll., on Inspection (Inspection Code), as amended). The Office does not deal with disputes
- between the controllers or the processors and data subjects or other natural or legal persons/entities arising from contractual or pre-contractual relations.

The Office is also responsible to deal with data subjects' complaints on unsolicited commercial messages under the Act on Certain Information Society Services (i.e., it receives and solve these complaints).

- Role, functions and powers of additional or ancillary data regulation authorities (if applicable): In the Czech Republic, the National Cyber and Information Security Agency (NÚKIB) supervises observance of the legal obligations laid down for the obliged persons by the Cyber Security Act.

The Czech Telecommunication Office is responsible to deal with data subjects' complaints against unsolicited marketing phone calls under the Act on Electronic Communications (i.e., it receives and solve these complaints).

8.3 Role, functions and powers of civil/criminal courts in the field of data regulation

The Czech civil courts deal with disputes between the controllers or the processors and data subjects or other natural or legal persons/entities arising from contractual or pre-contractual relations and also from the liability relations (damages).

The Czech administrative courts decide on administrative actions filed against decisions of the Czech administrative bodies/authorities, including the Office as mentioned in point 6.1 above.

The Czech criminal courts deal with crimes committed in the field of data protection, such as Unauthorised Use of Personal Data under section 180(2), Unauthorised Access to Computer Systems and Information Media under section 230(2) or Violation of Copyright, Rights Related to Copyright and Database Rights under section 270 of the Czech Penal Code (the Act no. 40/2009 Coll.).

Consequences of non-compliance

9.1 Consequences and penalties for data breach

Infringements of the GDPR are subject to administrative fines up to

EUR 20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

9.2 Consequences and penalties for other violations and non-compliance

If the Office finds that obligations imposed by the law have been breached, the Office will determine which measures must be adopted in order to eliminate the established shortcomings and set a deadline for their elimination. If the shortcomings are eliminated in accordance with the determined measures or immediately after the breach of obligation was found, the Office may decide not to impose fines. If the fines are imposed, mostly the general rules of the GDPR apply. Infringements of the GDPR are subject to administrative fines up to EUR 20,000,000, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

In case of commercial messages, legal entities may be fined up to CZK 10,000,000 (approximately EUR 405,000) for disseminating commercial communications in violation of the Certain Information Society Services Act. The Czech Office for Personal Data Protection (Office) is the authority for supervision of compliance with this act. In addition, fines and other

Czech Republic

measures may apply under the GDPR in case of breach of rules for processing of personal data (please see above).

Unsolicited/harassing phone calls (i.e., also marketing phone calls without consent unless the exception applies) are considered misdemeanour under the Act on Electronic communications. The Czech Telecommunication Office supervises compliance with the Czech Act on Electronic Communications, and has the authority to issue binding decisions, including prohibitions or orders and fines for violations. Legal entities may be fined up to CZK 50,000,000 (approximately EUR 2,022,000) or 10 % of the total worldwide annual turnover of the preceding financial year for unsolicited/harassing phone calls in violation of the Act on Electronic Communications.

Conclusion

The Czech Republic has implemented the GDPR mainly by the Act on Processing of Personal Data as mentioned above. There are also other laws that deal with the same or similar issues as the GDPR, but the GDPR stays the main law in the area of data protection and there are only very few additional requirements to and derivations from the GDPR in the Czech Republic.

As for the new legislation, it is expected that the new act on cyber security (likely to be effective in October 2024 in the Czech Republic) implementing the NIS 2 Directive will substantially broaden the number of entities to which this new Czech law will apply (from approx. 400 entities under the current law to approx. 6 000 entities under the new law).

THIS IS NOT LEGAL ADVICE.

This document provides general information on the current relevant legislation in the Czech Republic as of January 19, 2024. We remain at your entire disposal to analyse specific cases.

Contact Us

☎ +420 246 085 300

🌐 www.peterkapartners.com/

✉ hradil@peterkapartners.cz

📍 Karlovo náměstí 671/24
110 00 Praha 1