

GDPR

Local Implementation
in Central, Eastern &
Southeastern Europe

GDPR

Local Implementation in Central, Eastern & Southeastern Europe

This 2019 Wolf Theiss Guide, GDPR: Local Implementation in Central, Eastern & Southeastern Europe is intended as a practical guide to the general principles and features of the basic legislation and procedures in countries included in the publication.

While every effort has been made to ensure that the content is accurate when finalised, it should be used only as a general reference guide and should not be relied upon as definitive for planning or making definitive legal decisions. In these rapidly changing legal markets, the laws and regulations are frequently revised, either by amended legislation or by administrative interpretation.

Status of information: Current as of 1 May 2019

Conception, design, and editing:

WOLF THEISS Rechtsanwälte GmbH & Co KG, Attorneys-at-Law
Schubertring 6, 1010 Vienna, Austria
www.wolftheiss.com

TABLE OF CONTENTS

FOREWORD	04
GDPR AFTER(MATH)	05
COUNTRY CHAPTERS	08
AUSTRIA	08
BULGARIA	16
CROATIA	24
CZECH REPUBLIC	30
HUNGARY	37
POLAND	43
ROMANIA	49
SLOVAK REPUBLIC	56
SLOVENIA	62
OUR OFFICES	65

FOREWORD

We are pleased to present you with the first edition of the Wolf Theiss Guide, GDPR: Local Implementation in Central, Eastern and Southeastern Europe.

From the viewpoint of public awareness and practical enforcement, the EU General Data Protection Regulation (GDPR) has been the most important reform of European data protection laws in the last 25 years. At the same time, it sets international standards that go beyond the borders of the European Union and has led to similar initiatives in other countries around the world. Supplementing the GDPR, the member states still have to or may regulate certain aspects left to their local legal discretion. A year later, we take a look at what duties this law actually entails for companies and how member states and other countries have adapted their local data protection laws.

Wolf Theiss' strength has always been regional coverage. Our team of data protection experts are spread across the entire CEE/SEE region, giving our clients the advantage of seamless and efficient service across borders and specialised industry sectors to meet their business needs. This guide is intended to be a useful resource tool providing you with a brief overview of the differences between local laws in the CEE/ SEE region and the GDPR, and to answer some of the most frequently raised questions.

We hope that you will find the guide helpful. If you have any questions regarding the content or need more information, please do not hesitate to contact us or any of our regional team members listed in the guide.



Roland Marko

Partner, Wolf Theiss



Maria Maxim

Partner, Wolf Theiss



Kurt Retter

Partner, Wolf Theiss

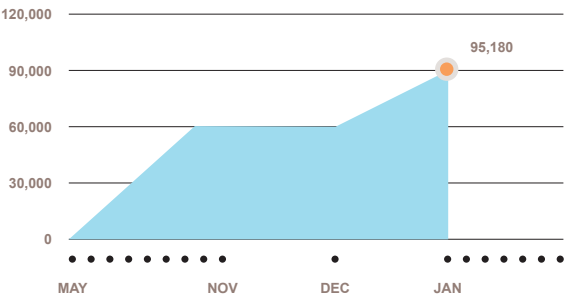
May 2019

GDPR AFTER(MATH) IN EUROPE

Since coming into force a year ago, the GDPR has seen a lot of activity under its provisions – here is a brief overview:

Complaints to the DPAs*:

Over the last year several complaints have been made to authorities all across Europe.



Most common type of complaints*:

Telemarketing and email spam seem to upset most.



Telemarketing



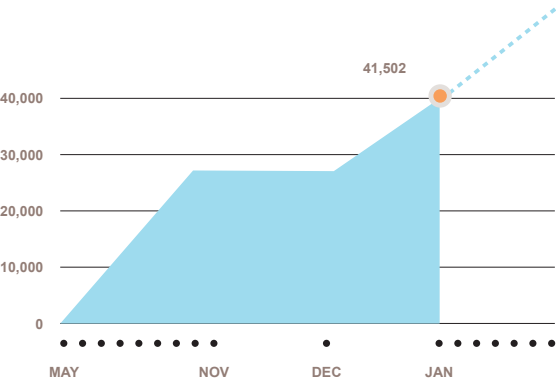
Promotional e-mails



Video surveillance/CCTV

Data breach notifications*:

Several companies have notified data breach incidents to the authorities.

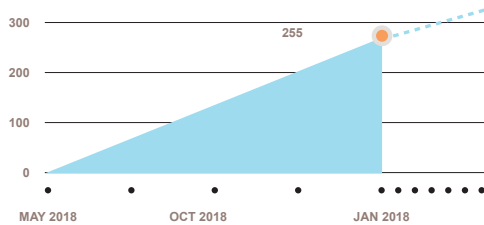


* Source: The European Commission (europa.eu/dataprotection) and the International Association of Privacy Professionals (GDPR One Year Anniversary)

GDPR AFTER(MATH) IN EUROPE

Cross- border cases*:

The global reach of companies has resulted in numerous cross-border cases.



Fines issued under the GDPR*:

While several cases are ongoing some of the fines that have been issued are:



For failure to comply with the information duty under Art. 14 GDPR: EUR 220,000

Unlawful video surveillance: EUR 5,280

For failure to secure users' data: EUR 20,000

Google for lack of consent: EUR 50,000,000

* Source: The European Commission (europa.eu/dataprotection) and the International Association of Privacy Professionals (GDPR One Year Anniversary)



EUROPE



- WOLF THEISS REGION
- EUROPE

AUSTRIA

NATIONAL IMPLEMENTING LEGISLATION IN A NUTSHELL

The prior Austrian Data Protection Act 2000 has been aligned with the GDPR through the Data Protection Amendment Act 2018 (*Datenschutz-Anpassungsgesetz 2018*) and the Data Protection Deregulation Act 2018 (*Datenschutz-Deregulierungsgesetz 2018*) (together, Austrian DPA, *österreichisches Datenschutzgesetz*). These changes include certain deviations from the GDPR which must be taken into account by companies, both, within their organisation (e.g. vis-à-vis employees) and externally (e.g. vis-à-vis customers) together with the GDPR.

Here, we highlight some of the most important provisions of the Austrian DPA that differ from the GDPR (e.g. data secrecy obligations, processing criminal data, age of child consent, etc)¹.

1. NATIONAL IMPLEMENTATION LAWS

1.1 Main Act

- ✂ **Data Protection Act / *Datenschutzgesetz***
Abb.: DSG

1.2 Other relevant laws

- ✂ **The General Data Protection Adjustment Act (*Materien-Datenschutz-Anpassungsgesetz 2018*)**
- ✂ **The research-sector-specific Data Protection Adjustment Act – Science and Research (*Datenschutz-Anpassungsgesetz 2018 – Wissenschaft und Forschung*)**
Abb.: WFDSAG 2018
- ✂ **Second General Data Protection Adjustment Act (2. *Materien-Datenschutz-Anpassungsgesetz 2018*)**

1.3 Relevant ordinances / Other guidelines

- ✂ **Black-List (*Datenschutz-Folgenabschätzung-Verordnung*)**
Abb.: DSFA-V
- ✂ **White-List (*Datenschutz-Folgenabschätzung-Ausnahmenverordnung*)**
Abb.: DSFA-AV

1 The additional laws adopted to implement provisions of the GDPR in other legal areas fall outside the scope of this guide. Some of these are:

- The General Data Protection Adjustment Act (*Materien-Datenschutz-Anpassungsgesetz 2018*)
- The research-sector-specific Data Protection Adjustment Act – Science and Research (*Datenschutz-Anpassungsgesetz 2018 – Wissenschaft und Forschung (WFDSAG 2018)*)
- Second General Data Protection Adjustment Act (2. *Materien-Datenschutz-Anpassungsgesetz 2018*)
- The DPIA Ordinance (DSFA-V), establishing the categories of processing operations that require a data protection impact assessment (so called “Black-List”)

The DPIA Exemptions Ordinance (DSFA-AV), determining the exemptions from the duty to carry out a data privacy impact assessment (so called “White-List”)

2. NATIONAL DATA PROTECTION AUTHORITY

🔗 **Austrian Data Protection Authority / Österreichische Datenschutzbehörde**
Abb.: DSB

3. NATIONAL IMPLEMENTATIONS / DEROGATIONS

GDPR	DSG	AUSTRIAN IMPLEMENTATION
Apart from Art. 9 GDPR, are there any further conditions or limitations for processing special categories of personal data?		
Art. 9(2) a, b, j; Art. 9(4)	N/A	No
Are there any additional authorisations required for processing personal data relating to criminal convictions/offences?		
Art. 10	§ 4 para 3	<p>The Austrian DPA permits processing personal data on acts or omissions punishable by courts or administrative authorities, including suspected criminal offenses and convictions, if the data controller satisfies each of the following conditions:</p> <ul style="list-style-type: none"> ▪ The processing meets the GDPR's requirements. ▪ The processing is based on: <ul style="list-style-type: none"> - an express legal authorization or obligation to process the data; or - statutory duties of diligence or necessity for the data controller or a third party to pursue their legitimate interests pursuant to GDPR Art. 6(1)(f) and the manner of processing safeguards the data subject's interests.
Apart from Art. 13, 14 GDPR, are there any further obligations, conditions, or exemptions from information duties?		
Art. 13 Art. 14	N/A	The Second General Data Protection Adjustment Act implements the GDPR in various sector specific laws. In the health sector, the application of, inter alia, Art. 13, 14 were excluded for e.g. doctors, hospitals, psychologist when processing patient data.
Apart from the regulations under the GDPR, are there any further obligations, conditions, or exemptions from data subject rights?		
Art. 17(1) Art. 17(3) Art. 22(2) Art. 23 Art. 89(2) Art. 89(3)	§ 4	<p>The Austrian DPA varies the following data subject rights or related data controller obligations when necessary to safeguard the GDPR Art. 23 objectives:</p> <p>i. Access Rights</p> <p>Under the Austrian DPA, the data subjects' access rights under GDPR Art. 15 do not apply if either:</p> <ul style="list-style-type: none"> ▪ Providing the information to the data subject jeopardizes the fulfillment of legally assigned tasks by a data controller exercising its powers as a public authority. ▪ Complying with the access request endangers trade or business secrets. <p>ii. Rectification and Erasure Rights</p> <p>The Austrian DPA also limits the data controller's obligation to rectify or erase personal data when the data controller uses automated data processing and can only carry out the rectification or erasure at certain times due to financial or technical constraints. In these cases, the data controller must restrict the personal data processing until the relevant time in compliance with GDPR Art. 18(2).</p> <p>When the data controller restricts personal data processing, it can only store the data or process it:</p> <ul style="list-style-type: none"> ▪ with the data subject's consent ▪ to establish, exercise, or defend legal claims ▪ to protect the rights of another individual or legal entity ▪ for important public interest reasons

GDPR	DSG	AUSTRIAN IMPLEMENTATION
Are there provisions that allow for the processing of data for secondary purposes (i.e. exceptions to the principle of purpose limitation in the case of a legal basis for processing)?		
Art. 6(4)	§ 10 § 7	<p>Secondary processing is permitted under limited circumstances. Organisations that lawfully process personal data may transfer the data to public-sector controllers and relief organisations if these entities need the personal data to manage a disaster. Public-sector controllers and relief organisations may jointly process the personal data to the extent necessary to:</p> <ul style="list-style-type: none"> assist those directly affected by the disaster find and identify deceased inform relatives <p>All other secondary processing must comply with the GDPR's requirements for secondary processing under GDPR Art. 6(4). For § 7 see below.</p>
Is there any change to the age of consent for children?		
Art. 8	§ 4 para 4	Yes, 14 years.
Are there additional obligations, conditions, or exemptions in connection with privacy impact assessments?		
Art. 35(10)	N/A	<p>No</p> <p>See only Austrian Black- and White-List (links above).</p>
Are there any further obligations, conditions, or exemptions in connection with data processing by a processor?		
Art. 28(3) Art. 28(4) Art. 29 Art. 32(4)	N/A	No
Are there any additional obligations when to appoint a data protection officer?		
Art. 37(4)	N/A	No
Are there additional obligations, conditions, or exemptions in connection with the transfer of data to a third country or an international organisation?		
Art. 49(1) Art. 49(5)	N/A	No
Are there additional limits on the transfer of specific categories of personal data to a third country or an international organisation?		
Art. 49(5)	N/A	No
In a nutshell, what are the local regulations in connection with the supervisory authority's powers, due process and remedies against actions and decisions of the local supervisory authority?		
Art. 58 Art. 83(8)	§ 30 § 11 § 22	<p>The principles of Austrian administrative law generally only allow fines to be imposed on natural persons, for example, the managing director or other representatives of the legal entity. However, to accommodate the high fines under the GDPR, the Austrian DPA also allows the Austrian Authority to impose administrative fines on legal persons under certain circumstances. For example, when a person acting individually or as part of an executive body infringes the GDPR or Austrian DPA, the Austrian Authority may fine the legal person when the acting individual has the authority to:</p> <ul style="list-style-type: none"> represent the legal person make decisions on behalf of the legal person exercise control within the legal person <p>The Austrian Authority may also hold legal persons responsible when the infringements were facilitated by a lack of supervision or control by persons in a position of authority within the legal person, unless the act is a criminal violation, punishable by the courts.</p>

GDPR	DSG	AUSTRIAN IMPLEMENTATION
		<p>The Austrian Authority should generally not impose a separate fine on a responsible manager or employee if it already imposed an administrative fine on the legal person for the same infringement.</p> <p>i.) The Austrian Authority must apply the criteria in GDPR Art. 83(2) to 83(6) when determining the amount of an administrative fine. It should ensure proportionality and primarily issue warnings instead of fines for first time offences.</p> <p>ii.) The Austrian DPA specifies the Austrian Authorities' powers in particular with respect to its right to inspection and the general obligation to protect the controller's rights and to official confidentiality regarding the information obtained (due process).</p> <p>iii.) Remedies can be filed according to the general administrative law.</p>
<p>Does a body, organisation or association have the right to: (i) lodge a complaint with the supervisory authority, (ii) sue for damages?</p> <p>Does this apply independently of a data subject's mandate, too? If so, which are these?</p>		
Art. 80(2)	§ 28	<p>i.) Yes</p> <p>ii.) Yes</p> <p>No, only on the data subject's instructions.</p>
<p>Are there modifications regarding sanctions (including criminal offences) for breach? Please explain, including amount of fines or imprisonment, etc.</p>		
Art. 84	§ 62 § 63	<p>i.) The Austrian DPA provides for further administrative offences punishable by fines of up to EUR 50,000. A punishable administrative offence is committed by anyone that:</p> <ul style="list-style-type: none"> Intentionally and illegally gains access to data processing or maintains an obviously illegal means of access. Intentionally transmits data in violation of the rules on confidentiality (found in Section 6, Austrian DPA). Intentionally and falsely pretending that certain facts are true in order to obtain personal data under Section 10 of the Austrian DPA that permits certain processing if a disaster occurs. Processes images in violation of the provisions regulating closed circuit television use under Section 12 of the Austrian DPA. Refuses inspection by the Austrian Authority. <p>ii.) Further, the use of data with the intention to make a profit or to cause harm constitutes a criminal offence punishable by a court with imprisonment of up to one year or a monetary penalty of up to 720 daily rates, unless the offence is subject to a more severe punishment under another provision.</p>
<p>Are there provisions to balance the protection of personal data with the rights to freedom of expression and information, including processing for journalistic, academic, artistic, or literary purposes?</p>		
Art. 85	§ 9	<p>i.) The Austrian DPA and several GDPR provisions do not apply to data processing by media owners, publishers, copy editors, or employees of media enterprises or media services within the meaning of the Austrian Media Act. The following Chapters of the GDPR do not apply to this type of processing:</p> <ul style="list-style-type: none"> Chapter II (Principles) Chapter III (Rights of the data subject) Chapter IV (Controller and processor) Chapter V (Transfer of personal data to third countries or international organisations). Chapter VI (Independent supervisory authorities) Chapter VII (Cooperation and consistency) Chapter IX (Provisions relating to specific processing situations) <p>ii.) Under the Austrian DPA, certain provisions of the GDPR do not apply to data processing for purposes of academic, artistic, or literary expression, if necessary to balance the data protection right with the freedom of expression and information.</p>

GDPR	DSG	AUSTRIAN IMPLEMENTATION
		<p>These GDPR provisions include:</p> <ul style="list-style-type: none"> Chapter II (Principles), except for Article 5 (Principles relating to processing of personal data), which continues to apply Chapter III (Rights of the data subject) Chapter IV (Controller and processor), except for Art. 28 (Processor), 29 (Processing under the authority of the controller or processor), and 32 (Security of processing) Chapter V (Transfer of personal data to third countries or international organisations) Chapter VI (Independent supervisory authorities) Chapter VII (Cooperation and consistency) Chapter IX (Provisions relating to specific processing situations) <p>iii.) In cases where these GDPR provisions do not apply to processing for purposes of academic, artistic, or literary expression, the Austrian DPA's data confidentiality provisions in Section 6 apply.</p>
Are there specific rules regarding data processing relating to employment?		
Art. 88	N/A	The Austrian DPA does not introduce more specific employment-related provisions. Instead, the general rules under employment law when processing employee data must be observed (shop agreement, consent requirements).
Are there specific rules regarding the processing of personal data for scientific or historic research, statistical purposes, big data operations, etc?		
Art. 89	§ 7	<p>i.) The Austrian DPA permits data controllers to process personal data for archiving purposes in the public interest or for scientific, historical research, or statistical purposes when the results obtained do not relate to specific data subjects. In these cases, the data controller may process:</p> <ul style="list-style-type: none"> publicly accessible personal data personal data collected by the data controller for other research projects or purposes pseudonymized personal data and the data controller cannot establish data subjects' identities <p>ii.) For all other processing for archiving purposes or for scientific, historical research, or statistical purposes, the data controller may only process personal data:</p> <ul style="list-style-type: none"> under specific legal provisions with the data subject's consent with a permit issued by the Austrian Data Protection Authority <p>iii.) The Austrian Data Protection Authority will grant a permit if all the following conditions apply:</p> <ul style="list-style-type: none"> The data controller cannot obtain the data subjects' consent because it is impossible to reach the data subjects or obtaining consent requires an unreasonable effort. There is a public interest in the data processing. The data controller has demonstrated its professional aptitude. <p>iv.) The sector-specific Data Protection Adjustment Act – Science and Research (in German) also includes provisions permitting processing for scientific purposes and implementing GDPR Art. 89. This sector-specific Act also restricts data subjects' rights under GDPR Art. 15 to 18, 20, and 21, if complying with the rights would make it impossible or seriously impact the scientific objectives. The requirements of this Act are outside the scope of this Guide.</p>
Any other relevant local law derogations to consider? (e.g. CCTV / video surveillance, provisions concerning the admissibility of processing of national identification numbers)		
Art. 87	§ 6	Data controllers, data processors, and their employees and persons in a quasi-employee relationship, must ensure the confidentiality of personal data entrusted to them or accessible by them solely due to their employment.

GDPR	DSG	AUSTRIAN IMPLEMENTATION
	§ 12, 13	<p>The Austrian DPA permits the use of video surveillance when:</p> <ul style="list-style-type: none"> ▪ It is necessary to protect the vital interests of a person. ▪ The data subject consents to the processing. ▪ Applicable law or other statutory provisions require or permit the processing. ▪ The data controller or a third party has an overriding legitimate interest in the processing and the processing is proportionate. <p>The Austrian DPA's specific requirements for using video surveillance are outside the scope of this Guide.</p>
<p>Are there any landmark decisions, material fines (including the underlying violation, eg violation of consent requirements), sector-focused investigations (e.g. banks, telecoms, health care) under the new law (GDPR or local DPA) to report so far?</p>		
<p>The highest fine so far that we are aware of amounted to EUR 4,800 for a violation of the provisions regarding the permissibility of image recordings (illegal video surveillance cameras). In many cases the authority did not impose a fine and instead only mandated specific amendments in data protection practices to achieve compliance.</p>		

This chapter was written by Roland Marko and Paulina Pomorski.



ROLAND MARKO
Partner

Wolf Theiss, Austria

T. +43 1 51510 5880
roland.marko@wolftheiss.com



PAULINA POMORSKI
Senior Associate

Wolf Theiss, Austria

T. +43 1 51510 5091
paulina.pomorski@wolftheiss.com

BULGARIA

NATIONAL IMPLEMENTING LEGISLATION IN A NUTSHELL

On 26 February 2019, the law amending and supplementing the Bulgarian Personal Data Protection Act (in Bulgarian: *Закон за изменение и допълнение на Закона за защита на личните данни*) in view of the GDPR ("**Implementing Law**") was published in the State Gazette. The Implementing Law has a twofold purpose – it implements the GDPR into national legislation and also transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data ("**Directive (EU) 2016/680**").

The Implementing Law does not reproduce the core provisions of the GDPR, such as the data processing principles and legal grounds for data processing. Instead, the Bulgarian legislator has adopted the approach of directly referring to the GDPR and introducing national rules complementary to the GDPR on matters that have not been explicitly covered by the regulation, or where the GDPR has left room for the exercise of legislative discretion.

The Implementing Law regulates, *inter alia*, the status and competences of local data protection authorities, the accreditation and certification in the field of personal data protection and the available legal remedies in case of violation of data protection legislations. Additional rules are also set with respect to certain specific data processing circumstances reflecting the practice under the former data protection framework.

Here we highlight the most important provisions of the Implementing Law which are within the framework of, but differ from, the GDPR¹.

1. NATIONAL IMPLEMENTATION LAWS

1.1 Main Act

- ⌘ **Personal Data Protection Act**
Abb.: PDPA

1.2 Relevant ordinances / Other guidelines

- ⌘ **Rules on the activity of the Commission for Personal Data Protection and its administration²**
- ⌘ **List of processing operations requiring data protection impact assessment pursuant to Art. 35(4) Regulation (EU) 2016/679**
- ⌘ **Guidelines on drafting and proposing a Code of Conduct in accordance with Art. 40 of Regulation (EU) 2016/679**
- ⌘ **Criteria and procedures for approving, amending or supplementing a Code of Conduct**

1 The provisions of the Implementing Law adopted for the purposes of transposing Directive (EU) 2016/680 into national legislation fall outside the scope of this guide.

2 The Implementing Law envisages amendment of the Rules on the activity of the Commission for Personal Data Protection ("Rules") and its administration to further regulate the competences and responsibilities of the CPDP under the GDPR. Currently, there is no publicly available information on the expected date for the adoption of the amended Rules.

NB: The Implementing Law envisages the adoption of secondary legislation to provide more detailed regulation on certain topics within the new data protection framework (e.g. requirements and procedure for granting accreditation of certifying bodies). Currently, there is no publicly available information on when such secondary legislation is to be expected.

2. NATIONAL DATA PROTECTION AUTHORITY

🔗 **Commission for Personal Data Protection**
 Abb.: CPDP
 English: <https://www.cdpd.bg/en/index.php?p=home&aid=0>

3. NATIONAL IMPLEMENTATIONS / DEROGATIONS

GDPR	PDPA	BULGARIAN IMPLEMENTATION
Apart from Art. 9 GDPR, are there any further conditions or limitations for processing special categories of personal data?		
Art. 9(2) a, b, j; Art. 9(4)	N/A	No
Are there any additional authorisations required for processing personal data relating to criminal convictions/offences?		
Art. 10	N/A	No
Apart from Art. 13, 14 GDPR, are there any further obligations, conditions, or exemptions from information duties?		
Art. 13 Art. 14	Art 25z (25з) para 3 and para 5 Art 25o (25о)	Yes, in cases where personal data is processed for journalistic purposes, or purposes of academic, artistic or literary expression the exercise of certain rights set out by the GDPR (including the information rights under Art. 13 and Art. 14) can be restricted. The exemption from the information requirements of the controller also applies to data processing for purposes of creating audio-visual or photographic works by way of filming/photographing a person in the course of his/ her public activities or at public places. Further Art. 12-22 (including the information rights under Art. 13 and Art. 14) and Art. 34 GDPR do not apply in cases where personal data is processed by public authorities and/or humanitarian organisations for humanitarian purposes, as well as to processing in case of natural disasters under the Disaster Protection Act.
Apart from the regulations under the GDPR, are there any further obligations, conditions, or exemptions from data subject rights?		
Art. 17(1) Art. 17(3) Art. 22(2) Art. 23 Art. 89(2) Art. 89(3) Art. 89(2) Art. 89(3)	Art 37a (37а) para 1 Art 25z (25з) para 3 and para 5 Art 25l (25л) Art 25m (25м) Art 25o (25о)	Data subjects may be denied (fully or partially) the right to exercise their rights set out in Art. 12-22 GDPR and the obligation under Art. 34 GDPR does not apply, when the exercise of such rights would constitute a risk to: <ul style="list-style-type: none"> ▪ national security ▪ defence ▪ public order and security ▪ the prevention, investigation, detection or prosecution of criminal offences or the enforcement of penalties, including the prevention of threats to public order and security ▪ in particular, an important economic or financial interest, including monetary, budgetary and fiscal matters, public health and social security ▪ the protection of the independence of the judiciary and judicial proceedings ▪ prevention, investigation, detection and prosecution of breaches of ethical codes in regulated professions ▪ the protection of the data subject or the rights and freedoms of others ▪ the enforcement of civil claims

GDPR	PDPA	BULGARIAN IMPLEMENTATION
		<p>The Implementing Law further excludes the application of Art. 6, 9, 10, 30 and 34 GDPR to processing for journalistic purposes, as well as for the purposes of academic, artistic or literary expression and limits the exercise of the data subjects' rights under Art. 12-22 GDPR and Art. 34 GDPR (see Question 3 above). Pursuant to the Implementing Law, Art. 6, 12-21, 30 and 34 GDPR shall not apply to data processing for the purposes of creating audio-visual or photographic works.</p> <p>Further derogations from the GDPR are envisaged in relation to personal data processing for the purposes of the National Archival Fund – under the Implementing Law in such cases the data subjects' rights set by Art. 15, 16, 18, 19, 20 and 21 GDPR shall not apply. Similarly, the Implementing Law grants a derogation from the rights under Art. 15, 16, 18 and 21 GDPR where personal data is processed for statistical purposes.</p> <p>Finally, the Implementing Law excludes the application of Art. 12-22 and Art. 34 GDPR to processing for humanitarian purposes and in case of natural disasters under the Disaster Protection Act.</p>
Are there provisions that allow for the processing of data for secondary purposes (i.e. exceptions to the principle of purpose limitation in the case of a legal basis for processing)?		
Art. 6(4)	Art 25n (25H)	<p>The Implementing Law allows for secondary processing for the purposes of the National Archival Fund, for the purposes of scientific or historical research and for statistical purposes. In such cases the data controller shall apply appropriate technical and organisational measures to secure the rights and freedoms of the data subjects in accordance with Art. 89(1) GDPR.</p> <p>All other secondary processing must comply with the GDPR's requirements for secondary processing under Art.6(4) GDPR.</p>
Is there any change to the age of consent for children?		
Art. 8	Art 25v (25B)	14 years
Are there additional obligations, conditions, or exemptions in connection with privacy impact assessments?		
Art. 35(10)	N/A	<p>No</p> <p>See only the list of processing operations requiring data protection impact assessment pursuant to Art. 35(4) of Regulation (EU) 2016/679 (link above).</p>
Are there any further obligations, conditions, or exemptions in connection with data processing by a processor?		
Art. 28(3) Art. 28(4) Art. 29 Art. 32(4)	N/A	No
Are there any additional obligations when to appoint a data protection officer?		
Art. 37(4)	N/A	No
Are there additional obligations, conditions, or exemptions in connection with the transfer of data to a third country or an international organisation?		
Art. 49(1) Art. 49(5)	N/A	No
Are there additional limits on the transfer of specific categories of personal data to a third country or an international organisation?		
Art. 49(5)	N/A	No
In a nutshell, what are the local regulations in connection with the supervisory authority's powers, due process and remedies against actions and decisions of the local supervisory authority?		
Art. 58 Art. 83(8)	Art 10 Art 10a Art 14a Art 15	<p>The Implementing Law defines the competences of the CPDP by directly referring to Art. 57 and 58 GDPR. In addition, the CPDP shall also be responsible for carrying out accreditation of certifying bodies and approving draft codes of conduct per sectors or per areas of activity. The CPDP shall further maintain public registers of: i) the data controllers/data processors that have appointed data protection officers; ii) the accredited certifying bodies; and iii) the approved codes of conduct under Art. 40 GDPR.</p>

GDPR	PDPA	BULGARIAN IMPLEMENTATION
	Art 84 Art 85 Art 38 Art 39	In case of established breaches of the European or local data protection legislation, shall be imposed fines (on natural persons) or pecuniary sanctions (on legal persons). The Implementing Law directly refers to the amounts of fines and pecuniary sanctions set out by the GDPR and the respective criteria for their determination. Under the Implementing law, in case of violation of the data subjects' rights set out by European or national data protection legislation, each data subject is entitled to refer the matter to the CPDP within six months of becoming aware of the breach, but no later than two years from the breach taking place. The decisions of the CPDP are subject to appeal before the Administrative Court Sofia within 14 days as of receipt in accordance with the rules of the Bulgarian Code of Administrative Procedure. The decisions of the Administrative Court-Sofia are subject to appeal before the Supreme Administrative Court, the decisions of which are final. A novelty in the Bulgarian data protection framework is the option for data subjects to challenge the actions and acts of the data controller/processor directly before the administrative courts. This option, however, is not applicable in case there are pending proceedings before the CPDP for the same matter, or if a decision regarding the same breach has been appealed against and no corresponding court decision has entered into force.
Does a body, organisation or association have the right to: (i) lodge a complaint with the supervisory authority, (ii) sue for damages? Does this apply independently of a data subject's mandate, too? If so, which are these?		
Art. 80(2)	N/A	No
Are there modifications regarding sanctions (including criminal offences) for breach? Please explain, including amount of fines or imprisonment, etc.		
Art. 84	Art 86	The Implementing Law stipulates that other violations of the national data protection legislation (i.e. besides the violations set by the GDPR and referred to by the Implementing Law) shall be sanctioned with a fine/pecuniary sanction of up to BGN 5,000 (approx. EUR 2,500). The sanction for repeated violations shall be up to twice the amount of the initially imposed fine/pecuniary sanction.
Are there provisions to balance the protection of personal data with the rights to freedom of expression and information, including processing for journalistic, academic, artistic, or literary purposes?		
Art. 85	Art 25z (253)	Under the Implementing Law data processing for journalistic, academic, artistic or literary purposes is only lawful when: i) it is carried out in the context of exercising the freedom of expression and the right to information; and ii) the privacy and personal life of the data subjects are respected. The Implementing Law sets out the following list of criteria to be considered and observed to assess the balance between the freedom of expression and right to information on the one hand, and the protection of privacy on the other: i.) the nature of the personal data concerned ii.) the impact a public disclosure of the personal data would have on the privacy of the data subject and his/her reputation iii.) the circumstances under which the personal data has become known to the data controller iv.) the form and essence of the statement by which the freedom of expression and information has been exercised v.) the importance of the public disclosure of personal data for clarifying a matter of public interest vi.) whether the data subject is a person who holds a position under Art. 6 of the Counter-Corruption and Unlawfully Acquired Assets Forfeiture Act or whether a person, who due to the nature of his / her activity or role in public life, has a lesser degree of protection of his / her privacy or whose actions have an impact on society vii.) whether the data subject has contributed to the disclosure of his/her personal data and/ or information on his/ her personal and family life; the purpose, content, form and consequences of the statement by which the freedom of expression and information has been exercised viii.) the compliance of the statement by which the freedom of expression and information has been exercised with fundamental civil rights

GDPR	PDPA	BULGARIAN IMPLEMENTATION
	Art 25j (25ж) Art 25g (25r)	<p>iii. Processing of personal identification number and copying of identification documents</p> <p>The Implementing Law prohibits free public access to personal identification number and personal identification number of a foreigner (PIN/PINF), unless provided for by law. Data controllers providing e-services should implement appropriate technical and organisational measures to prevent the PIN/PINF from being the sole identifier used for remote access to such services.</p> <p>Controllers/processors can lawfully copy data subjects' identification documents, driving license or residence documents only when explicitly provided for by law.</p>
<p>Are there any landmark decisions, material fines (including the underlying violation, eg violation of consent requirements), sector-focused investigations (e.g. banks, telecoms, health care) under the new law (GDPR or local DPA) to report so far?</p> <p>In February 2019, the CPDP imposed the first significant sanction for the violation of the GDPR in the amount of BGN 53,000 (approx. EUR 26,000). The sanction was imposed on a mobile operator for violation of the principles of processing of personal data, including the requirements for consent for data processing. A subscriber of the mobile operator established that his subscription plan was transformed into a contract for prepaid services without his knowledge or consent.</p> <p>In its decision, the CPDP indicates that the high amount of the sanction is due to the repeated violations of data protection rules committed by this particular mobile operator (including for the same infringement), for which the CPDP has already sanctioned the latter several times.</p>		

This chapter was written by Anna Rizova and Zhulieta Markova.



ANNA RIZOVA
Partner

Wolf Theiss, Bulgaria

T. +359 2 8613 703
anna.rizova@wolftheiss.com



ZHULIETA MARKOVA
Senior Associate

Wolf Theiss, Bulgaria

T. +359 2 8613 731
zhulieta.markova@wolftheiss.com

CROATIA

NATIONAL IMPLEMENTING LEGISLATION IN A NUTSHELL

The GDPR has been introduced into the Croatian legal system through the Law on Implementation of the General Data Protection Regulation (Croatian: *Zakon o provedbi Opće uredbe o zaštiti podataka*; “ZPGDPR”).

The ZPGDPR primarily regulates the composition and powers of the Croatian regulator – being the Croatian Personal Data Protection Agency (“AZOP”) and also provides for some specific provisions related to certain types of data processing or processing of certain data categories (e.g., biometric data and video surveillance). However, the Croatian legislator did not use many derogation possibilities provided under the GDPR, which is why in most of the situations the provisions of GDPR will be directly applicable.

Besides, based on its authority as regulator given under Art. 35(4) GDPR, the AZOP established a list of processing operations which are subject to the requirement of the performance of a data protection impact assessment (PIA).

1. NATIONAL IMPLEMENTATION LAWS

1.1 Main Act

- 🔗 **Law on Implementation of the General Data Protection Regulation (Croatian: *Zakon o provedbi Opće uredbe o zaštiti podataka*), Official Gazette of the Republic of Croatia, No. 42/18**
Abb.: ZPGDPR

1.2 Other relevant law

- 🔗 **Decision of a list of processing operations which are subject to the requirement of a data protection impact assessment, rendered by the regulator based on its authority given under Art 35(4) GDPR (so called Black-List)**

2. NATIONAL DATA PROTECTION AUTHORITY

- 🔗 **Croatian Personal Data Protection Agency (Croatian: *Agencija za zaštitu osobnih podataka*)**
Abb.: AZOP

3. NATIONAL IMPLEMENTATIONS / DEROGATIONS

GDPR	ZPGDPR	CROATIAN IMPLEMENTATION
Apart from Art. 9 GDPR, are there any further conditions or limitations for processing special categories of personal data?		
Art. 9(2) a, b, j; Art. 9(4)	Art. 20-24	<p>Yes</p> <p>They are:</p> <p>i. Processing of genetic data:</p> <ul style="list-style-type: none"> ▪ Processing of genetic data for the purpose of calculation of disease occurrence probability or other health aspects of data subjects within activities related to conclusion or execution of life insurance contracts or pure endowment clauses is prohibited (cannot be processed even if there is explicit prior consent by the data subject). ▪ This limitation applies to data subjects that conclude life insurance contracts or contracts including pure endowment clauses in the Republic of Croatia if the data processing is carried out by a data controller that is established in the Republic of Croatia or that provides services within the Republic of Croatia.

GDPR	ZPGDPR	CROATIAN IMPLEMENTATION
		ii. Processing of biometric data: <ul style="list-style-type: none"> Processing of biometric data is allowed only if determined by law or if it is necessary for the protection of persons, property, classified data or business secrets, but always taking into account that the data subject's interests are not contrary to such processing. Additionally, private entities are allowed to process biometric data for safe identification of services' users, but only subject to explicit prior consent given in accordance with the provisions of the GDPR. Processing of employees' biometric data with the purpose of evidencing working hours and enabling entrance/ exit from the business premises is allowed if determined by law or if it is an alternative to another solution for evidencing working hours and enabling entrance/ exit from the business premises. This must always be subject to explicit prior consent given in accordance with the provisions of the GDPR. The above limitations apply to data subjects in the Republic of Croatia if the data processing is carried out by a data controller established or providing services in the Republic of Croatia or by public body.
Are there any additional authorisations required for processing personal data relating to criminal convictions/offences?		
Art. 10	N/A	No
Apart from Art. 13, 14 GDPR, are there any further obligations, conditions, or exemptions from information duties?		
Art. 13 Art. 14	N/A	No
Apart from the regulations under the GDPR, are there any further obligations, conditions, or exemptions from data subject rights?		
Art. 17(1) Art. 17(3) Art. 22(2) Art. 23 Art. 89(2) Art. 89(3)	Art. 33	No However, public bodies that process data for official statistical purposes are not obliged to ensure rights to access, rectification, restriction or objection of processing.
Are there provisions that allow for the processing of data for secondary purposes (i.e. exceptions to the principle of purpose limitation in the case of a legal basis for processing)?		
Art. 6(4)	N/A	No
Is there any change to the age of consent for children?		
Art. 8	Art. 19	No Processing of data of minors residing in Croatia in relation to information society is lawful only if the child is at least 16 years old.
Are there additional obligations, conditions, or exemptions in connection with privacy impact assessments?		
Art. 35(10)	N/A	No See only Black-List (link above).
Are there any further obligations, conditions, or exemptions in connection with data processing by a processor?		
Art. 28(3) Art. 28(4) Art. 29 Art. 32(4)	N/A	No
Are there any additional obligations when to appoint a data protection officer?		
Art. 37(4)	N/A	No

GDPR	ZPGDPR	CROATIAN IMPLEMENTATION
Are there additional obligations, conditions, or exemptions in connection with the transfer of data to a third country or an international organisation?		
Art. 49(1)	N/A	No
Art. 49(5)		
Are there additional limits on the transfer of specific categories of personal data to a third country or an international organisation?		
Art. 49(5)	N/A	No
In a nutshell, what are the local regulations in connection with the supervisory authority's powers, due process and remedies against actions and decisions of the local supervisory authority?		
Art. 58 Art. 83(8)	Section III Section V	The composition and authorities of the AZOP are regulated by the ZPGDPR. Generally, the AZOP is responsible for monitoring and protecting fundamental rights relating to data processing. Besides powers awarded directly by the GDPR, the AZOP is conferred with additional competences such as the right to participate in court proceedings, issue criteria for determining the amount of administrative compensation, publish decisions and opinions, etc. In case of violation, AZOP is authorized to impose administrative fines prescribed by the GDPR and/or ZPGDPR (please see Section 10 below). AZOP's decisions are not directly appealable but may be challenged in court proceedings held before the administrative courts.
Does a body, organisation or association have the right to: (i) lodge a complaint with the supervisory authority, (ii) sue for damages? Does this apply independently of a data subject's mandate, too? If so, which are these?		
Art. 80(2)2	N/A	No
Are there modifications regarding sanctions (including criminal offences) for breach? Please explain, including amount of fines or imprisonment, etc.		
Art. 84	Art. 50 Art. 51 Art. 47	In addition to administrative fines under the GDPR, the ZPGDPR provides for: <ul style="list-style-type: none"> ▪ misdemeanor fines of up to HRK 50,000 (approx. EUR 6,700) for violations made by the AZOP's workers; and ▪ administrative fines of up to HRK 50,000 (approx. EUR 6,700) for violations related to video surveillance. State administrative bodies are not subject to fines under the GDPR and/or ZPGDPR.
Are there provisions to balance the protection of personal data with the rights to freedom of expression and information, including processing for journalistic, academic, artistic, or literary purposes?		
Art. 85	N/A	No
Are there specific rules regarding data processing relating to employment?		
Art. 88	N/A	Yes, with regard to the video surveillance of employees. Please see the answer to the question on video surveillance below.
Are there specific rules regarding the processing of personal data for scientific or historic research, statistical purposes, big data operations, etc?		
Art. 89	N/A	Public bodies which process data for official statistical purposes are not obliged to ensure rights to access, rectification, right to restriction of processing, right to object to processing and right to complain. When transferring personal data to public bodies in order for them to perform processing for the purpose of official statistics, controllers are not obliged to notify data subjects about such transfers. Personal data processed for statistical purposes shall be anonymized, i.e., shall not allow the identification of the person to whom the data relates.
Any other relevant local law derogations to consider? (e.g. CCTV / video surveillance, provisions concerning the admissibility of processing of national identification numbers)		
Art. 87	N/A	Video surveillance may be performed only for a purpose that is necessary and justified in order to protect persons and assets, if it is not contrary to prevalent interests of the data subject.

GDPR	ZPGDPR	CROATIAN IMPLEMENTATION
		<p>Information about the video surveillance must be available before the person is stepping within the perimeter of video surveillance and needs to contain all relevant information pursuant to Art. 13 GDPR, and a simple easy to understand diagram.</p> <p>Additional requirements may apply in specific situations (e.g. in the employment context, business-residential buildings, public areas)</p>
Are there any landmark decisions, material fines (including the underlying violation, eg violation of consent requirements), sector-focused investigations (e.g. banks, telecoms, health care) under the new law (GDPR or local DPA) to report so far?		
No		

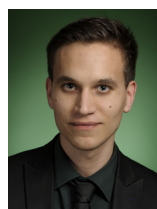
This chapter was written by Luka Tadic-Colic and Ivan Zornada.



LUKA TADIC-COLIC
Partner

Wolf Theiss, Croatia

+385 1 4925 436
luka.tadic-colic@wolftheiss.com



IVAN ZORNADA
Associate

Wolf Theiss, Croatia

+385 1 4925 422
ivan.zornada@wolftheiss.com

CZECH REPUBLIC

NATIONAL IMPLEMENTING LEGISLATION IN A NUTSHELL

On 12 March 2019, the Czech Republic approved a legislation incorporating the provisions of the GDPR. The Chamber of Deputies approved the final version of the bill Data Processing Act (DPA) repealing the previous Act No. 101/2000 Coll., on Personal Data Protection, that was partly inapplicable from the day the GDPR came into force (25 May 2018).

Here, we highlight the most important provisions of the Czech DPA that differ from the GDPR (for instance, age of child consent, possibilities for restricting data subjects' rights in matters of public interest and regarding the enforcement of private claims, possibility of informing data subjects online when data processing is based on law and in the public interest.

Several other laws will also have to be amended.¹

1. NATIONAL IMPLEMENTATION LAWS

1.1 Law

- 🔗 **Bill on Personal Data Processing / *Návrh zákona o zpracování osobních údajů***
Abb.: DPA

1.2 Other relevant laws

- 🔗 **Bill amending certain acts in relation to the Act on Personal Data Processing / *Návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o zpracování osobních údajů***
Abb.: Amending Act
- 🔗 **Act No. 101/2000 Coll., on Personal Data Protection / *Zákon o ochraně osobních údajů***
Abb.: Former DPA

1.3 Relevant ordinance / Other guideline

- 🔗 **Non-binding draft of a list of personal data processing operations that are not subject to a privacy impact assessment issued by the Czech Office for Personal Data Protection (so called "White-List") / *Návrh seznamu operací zpracování osobních údajů, která nepodléhají posouzení vlivu na ochranu osobních údajů***
Abb.: DPIA White-List

¹ Among others, these include:

- Czech Act No. 141/1961 Coll., Criminal Procedure Code, as amended,
- Czech Act No. 99/1963 Coll., Civil Procedure Code, as amended,
- Czech Act No. 106/1999 Coll., on Free Access to Information, as amended,
- Czech Act No. 273/2008 Coll., on Police of the Czech Republic, as amended,
- Czech Act No. 280/2009 Coll., Tax Code, as amended,
- Czech Act No. 269/1994 Coll., on the Criminal Registry, as amended,
- Czech Act No. 48/1997 Coll., on Public Health Insurance, as amended.

2. NATIONAL DATA PROTECTION AUTHORITY

🔗 **The Office for Personal Data Protection**
Abb.: OPDP

3. NATIONAL IMPLEMENTATIONS / DEROGATIONS

GDPR	DPA	CZECH IMPLEMENTATION
Apart from Art. 9 GDPR, are there any further conditions or limitations for processing special categories of personal data?		
Art. 9(2) a, b, j; Art. 9(4)	Section 16(2)	<p>Yes</p> <p>Special categories of personal data may be processed for scientific or historic research or statistical purposes provided that specific measures are adopted to protect the data subject's interests and that the data are processed in a way that does not allow identification of the data subject and the legitimate interests of the data subject does not override such processing.</p> <p>In addition, special categories of personal data may be processed pursuant to other laws, for example under Labour, Banking, Health, Education and State Security laws.</p>
Are there any additional authorisations required for processing personal data relating to criminal convictions/offences?		
Art. 10	N/A	<p>Not, in the DPA.</p> <p>Yet, there are several special acts that require the employer to obtain criminal records of employees, in particular in the area of Education, State Security, Municipal Police, Military Forces etc.</p>
Apart from Art. 13, 14 GDPR, are there any further obligations, conditions, or exemptions from information duties?		
Art. 13 Art. 14	Section 8 See also clause 4 below.	<p>Yes</p> <p>When the controller processes personal data</p> <ul style="list-style-type: none"> to comply with legal obligations to which the controller is subject, for the performance of a task carried out in the public interest in the exercise of official authority vested in the controller <p>the controller may provide the data to the data subject by remote access, i.e., electronically.</p>
Apart from the regulations under the GDPR, are there any further obligations, conditions, or exemptions from data subject rights?		
Art. 17(1) Art. 17(3) Art. 22(2) Art. 23	Section 5	<p>The Controller may process the data if it is necessary to:</p> <ul style="list-style-type: none"> comply with legal obligations to which the controller is subject perform a task carried out in the public interest or in the exercise of official authority vested in the controller
Art. 89(2) Art. 89(3)	Section 9 Section 11	<p>The obligation to inform about corrections, limitations or erasure of personal data may be fulfilled by updating the initial records that are available to the data subject.</p> <p>The obligations of the controller/processor (set out in Art. 5 and Art. 12-22 GDPR) shall be applied proportionately or postponed when necessary and adequate to prevent a serious threat to protected objections² defined in Section §6(2) DPA. The controller will have to notify the Authority about the above without undue delay and provide adequate extent information under Art. 23(2) GDPR.</p>

² Protected objection under Section 6(2) DPA means particularly defense/security of the Czech Republic; public order, internal security; prevention, investigation, detection of criminal activities, prosecution of criminal offences or enforcement of criminal penalties; other public interest objective of the EU/Member State (such as monetary, fiscal, tax, public health and social security); protection of judiciary independence and of judicial proceedings; prevention, investigation, detection or prosecution of ethical rules violations of regulated professions; or monitoring, inspection or regulatory functions linked, even occasionally, to the exercise of official authority in the cases referred to in points above; protection of the rights and freedoms of a data subject persons, or the enforcement of private claims.

GDPR	DPA	CZECH IMPLEMENTATION
	Section 12	A notification of the data breach to the data subject shall be limited or postponed if it is adequate and necessary to prevent a threat to protected objections defined in Section §6(2) DPA.
	Sections 18, 19, 20(1), 22, 23	<p>Processing for journalistic, academic, artistic, or literary purposes includes certain derogations from data subjects' rights and information requirements:</p> <p>The controller may comply with its obligations under Art. 12(1), 2, Art. 13 (1-3,) Art. 21 (4) and Art. 5 GDPR to the corresponding extent, by informing the data subject about the identity of the controller in any appropriate means (by graphic labelling, verbally etc.). Information about identity is sufficient if the information duty of the controller about the data subject's rights and other information is publicly available online.</p> <ul style="list-style-type: none"> ▪ The controller does not have to provide the source of the personal data. ▪ The right to object is available only in specific cases where the data subject must be able to prove that their legitimate interest on the protection of their rights and freedoms overrides. ▪ Rights of data subjects and notice obligations of the controller may be excluded, proportionally limited or postponed if it is needed for the fulfillment of such purposes and if it does not pose a high risk to data subjects' legitimate interests.
Are there provisions that allow for the processing of data for secondary purposes (i.e. exceptions to the principle of purpose limitation in the case of a legal basis for processing)?		
Art. 6(4)	Section 6	<p>Yes</p> <p>The controller processing personal data to secure protected objectives shall not be obliged to assess compatibility of those purposes and the purpose for which the personal data was initially collected if the processing is necessary and proportionate for:</p> <ul style="list-style-type: none"> ▪ the fulfillment of a legal obligation imposed on the controller ▪ performance of a task carried out in the public interest or in the exercise of official authority vested in the controller
Is there any change to the age of consent for children?		
Art. 8	Section 7	Yes, 15 years
Are there additional obligations, conditions, or exemptions in connection with privacy impact assessments?		
Art. 35(10)	Section 10	<p>No</p> <p>The DPA expressly stipulates an exemption from Art. 35(10) GDPR stating that a controller does not have to carry out privacy impact assessments when a law requires him to perform such data processing.</p> <p>In addition, there is a non-binding White-List issued by the OPDP.</p>
Are there any further obligations, conditions, or exemptions in connection with data processing by a processor?		
Art. 28(3) Art. 28(4) Art. 29 Art. 32(4)	Section 34	Yes, but only with respect to data processing by public authorities for concerns regarding criminal activity, security and public order in the Czech Republic.
Are there any additional obligations when to appoint a data protection officer?		
Art. 37(4)	Section 14	<p>Yes</p> <p>In addition to public authorities, bodies that fulfill tasks designated by law to be in the public interest are obliged to appoint a Data Protection Officer.</p>
Are there additional obligations, conditions, or exemptions in connection with the transfer of data to a third country or an international organisation?		
Art. 49(1) Art. 49(5)	N/A	No
Are there additional limits on the transfer of specific categories of personal data to a third country or an international organisation?		
Art 49(5)	N/A	No

GDPR	DPA	CZECH IMPLEMENTATION
In a nutshell, what are the local regulations in connection with the supervisory authority's powers, due process and remedies against actions and decisions of the local supervisory authority?		
Art. 58 Art. 83(8)	Title V. and VI.	<p>The OPDP is a central administrative body for the protection of personal data. It monitors data processing and controls compliance with the data protections laws. It:</p> <ul style="list-style-type: none"> i.) performs audits ii.) enforces subjects to abide by the regulation iii.) informs the controllers and processors about their obligations and duties in the area of personal data protection iv.) warns them about possible violations of the law v.) approves codes of conduct vi.) deals with offences and imposes fines vii.) provides consulting in the area of personal data protection viii.) provides the Czech Parliament with statements regarding new regulations on the processing of personal data and ix.) ensures compliance with treaties and legislations of the European Union <p>The OPDP gained new powers in the area of free access to information. The OPDP may for instance issue (a directly enforceable) instruction to subordinate authorities to provide information.</p>
Does a body, organisation or association have the right to: (i) lodge a complaint with the supervisory authority, (ii) sue for damages? Does this apply independently of a data subject's mandate, too? If so, which are these?		
Art. 80(2)	N/A	Yes, but only on the data subject's instructions.
Are there modifications regarding sanctions (including criminal offences) for breach? Please explain, including amount of fines or imprisonment, etc.		
Art. 84	Section 61, 62, 63	<p>Yes</p> <p>The DPA differentiates among the following three general types of administrative offences that may be committed by individuals, legal entities or individuals conducting a business:</p> <ul style="list-style-type: none"> i.) offences of breaching a prohibition of personal data disclosure imposed by another legal regulation that may be subject to a fine up to CZK 1,000,000 (approx. EUR 40,000); ii.) offences under (i) above may be subject to a fine up to CZK 5,000,000 (approx. EUR 200,000) if committed via press, television, radio, public computer networks, etc. iii.) offences stipulated in Section 63 of DPA that may be subject to a fine of up to CZK 10,000,000 (approx. EUR 400,000); <p>The OPDP shall refrain from imposing an administrative penalty if it concerns public authorities and bodies under Art 83(7) GDPR.</p> <p>The Criminal Code sets out additional sanctions³.</p>
Are there provisions to balance the protection of personal data with the rights to freedom of expression and information, including processing for journalistic, academic, artistic, or literary purposes?		
Art. 85	Section 17	Data processing for journalistic, academic, artistic or literary purposes is permissible when proportionate.
Are there specific rules regarding data processing relating to employment?		
Art. 88	N/A	<p>No</p> <p>The DPA does not introduce more specific employment related provisions. Instead, the general rules under employment laws must be complied with when processing employees' data.</p>

³ Section 180 of the Act No. 40/2009 Coll., Criminal Code; Section 8(5) of the Act No. 418/2011 Coll., Legal Persons Criminal Liability Act

GDPR	DPA	CZECH IMPLEMENTATION
Are there specific rules regarding the processing of personal data for scientific or historic research, statistical purposes, big data operations, etc?		
Art. 89	Section 16	<p>Controllers/ processors must ensure technical and organisational measures, record keeping, the appointment of a data protection officer etc. when processing data for scientific or historic research or statistical purposes in order to protect the data subject's interests.</p> <p>It is possible to process special categories of personal data for scientific or historic research or statistical purposes provided that the data are processed in a way that do not allow the identification of the data subject and the legitimate interests of the data subject does not override such processing.</p> <p>The data subject's rights to access, rectification, restriction and objecting may be adequately limited or postponed if it is necessary for scientific or historic research or statistical purposes.</p>
Any other relevant local law derogations to consider? (e.g. CCTV / video surveillance, provisions concerning the admissibility of processing of national identification numbers)		
Art. 87	N/A	<p>No, the DPA does not determine any derogations.</p> <p>National identification numbers (birth certificate numbers) may be processed for the purpose of enforcing private claims⁴.</p>
Are there any landmark decisions, material fines (including the underlying violation, eg violation of consent requirements), sector-focused investigations (e.g. banks, telecoms, health care) under the new law (GDPR or local DPA) to report so far?		
<p>There have been no significant fines so far. The largest GDPR fines imposed till date by the Czech Data Protection Authority were approximately CZK 30,000 (EUR 1,100). One was for failing to secure contracts with client details and the other was for GPS use in company cars.</p>		

4 (Section 13 para c) of Act No. 133/2000 Coll., Population Registration Act)

This chapter was written by Jitka Logesova and Katerina Kulhankova.



JITKA LOGESOVA

Partner

Wolf Theiss, Czech Republic

T. +420 234 765 223

jitka.logesova@wolftheiss.com



KATERINA KULHANKOVA

Senior Associate

Wolf Theiss, Czech Republic

T. +420 234 765 252

katerina.kulhankova@wolftheiss.com

HUNGARY

NATIONAL IMPLEMENTING LEGISLATION IN A NUTSHELL

On 25 July 2018, the Act XXXVIII of 2018 on the amendment of the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information (“**Hungarian DPA**”) in connection with the data protection reform of the European Union and the amendment of corresponding laws (in Hungarian: *2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról*) (“**Implementing Law**”) was published in the Official Gazette to transpose and harmonise the provisions of the GDPR into national law.

The Implementing Law regulates, *inter alia*, the status and competences of the local data protection authority and the available legal remedies in case of violation of the data protection legislation. Additional rules are also set with respect to certain specific data processing circumstances reflecting the practice under the former data protection framework.

Besides the Implementing Law another important piece of legislation was promulgated on 11 April 2019. The Act XXXIV. of 2019 on amendment of certain acts in connection with the execution of the data protection reform of the European Union (in Hungarian: *2019. évi XXXIV. törvény az Európai Unió adatvédelmi reformjának végrehajtása érdekében szükséges törvénymódosításokról*) (“**Execution Act**”). It covers 86 sectorial regulations.¹

Here, we highlight the most important provisions of the Implementing Law which are within the framework of but differ from the GDPR.

1. NATIONAL IMPLEMENTATION LAWS

1.1 Main Act

- ⌘ **Hungarian National Authority for Data Protection and Freedom of Information**
Abb.: DPA

1.2 Other relevant laws

- ⌘ **Act XXXVIII of 2018 on the amendment of the Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information in connection with the data protection reform of the European Union and the amendment of corresponding laws**
- ⌘ **Act XXXIV. of 2019 on amendment of certain acts in connection with the execution of the data protection reform of the European Union**

1.3 Relevant ordinances / Other guidelines

- ⌘ **List of processing operations requiring data protection impact assessment pursuant to Art. 35(4) of Regulation (EU) 2016/679 (so called Black list)**
- ⌘ **Statements in connection with the application of the GDPR**

1 The Execution Act will amend (enter into force on 26 April 2019), among others

- the Labour Code (Act I of 2012 on the Labour Code)
- the Act CXXXIII of 2005 on Security Services and the Activities of Private Investigators
- Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing
- ACT XLVII of 1997 on the Processing and Protection of Health – and Connected Personal Data

NATIONAL DATA PROTECTION AUTHORITY

♂ Hungarian National Authority for Data Protection and Freedom of Information

Abb.: NAIH

2. NATIONAL IMPLEMENTATIONS / DEROGATIONS

GDPR	DPA	HUNGARIAN IMPLEMENTATION
Apart from Art. 9 GDPR, are there any further conditions or limitations for processing special categories of personal data?		
Art. 9(2) a, b, j; Art. 9(4)	Art. 5 (7)	Yes The DPA provides that some of its provisions shall apply in parallel to the provisions of the GDPR. For instance, it states that: The processing of personal data processed in criminal matters and the provisions on the processing of sensitive data shall apply unless an act, an international treaty or a binding legislation of the European Union provides otherwise.
Are there any additional authorisations required for processing personal data relating to criminal convictions/offences?		
Art. 10	Art. 5 (4)	Yes. According to the DPA, the following category of data can only be processed only by central or local government authorities: <ul style="list-style-type: none"> personal data from the criminal records which are processed for the purpose of prevention, investigation and prosecution of criminal activities and for administrative and law enforcement purposes data files containing information pertaining to misdemeanour cases, civil cases and non-contentious proceedings, and for contentious and non-contentious administrative proceedings
Apart from Art. 13, 14 GDPR, are there any further obligations, conditions, or exemptions from information duties?		
Art. 13 Art. 14	N/A	The Execution Act implements the GDPR in various sector specific laws. In the health sector, the fee of further copies requested by the data subject is set out in a ministerial decree. In case of employment relationships, the employer should provide the information set out in Art. 13 of the GDPR in writing. (Health Data Act and Labour Code)
Apart from the regulations under the GDPR, are there any further obligations, conditions, or exemptions from data subject rights?		
Art. 17(1) Art. 17(3) Art. 22(2) Art. 23 Art. 89(2) Art. 89(3)	Section 5 (8)	The DPA allows bodies or persons conducting scientific research to disclose personal data if it is necessary to demonstrate the findings of research in connection with historical events
Are there provisions that allow for the processing of data for secondary purposes (i.e. exceptions to the principle of purpose limitation in the case of a legal basis for processing)?		
Art. 6(4)	N/A	No
Is there any change to the age of consent for children?		
Art. 8	N/A	No The age of consent is 16 years.
Are there additional obligations, conditions, or exemptions in connection with privacy impact assessments?		
Art. 35(10)	Section 25/G (3)-(4)	According to the DPA if the Authority establishes that a specific type of data processing operation involves a high risk and makes such public finding [according to Art. 35(4)], all envisaged data processing shall be presumed to result in a high risk which includes the same or similar type of data processing operation.

GDPR	DPA	HUNGARIAN IMPLEMENTATION
		<p>Similarly, if the Authority establishes that a specific type of data processing operation does not involve a high risk and makes such public finding, any envisaged data processing that involves the use of data processing operations that are considered to be the same or similar to the type of data processing operation in question such processing shall be presumed not to result in a high risk.</p> <p>Please see the Hungarian "Black –List" according to Art. 35 (4) GDPR (link above).</p>
Are there any further obligations, conditions, or exemptions in connection with data processing by a processor?		
Art. 28(3) Art. 28(4) Art. 29 Art. 32(4)	N/A	No
Are there any additional obligations when to appoint a data protection officer?		
Art. 37(4)	Art. 25/M (2) and 25/N	<p>The data protection officer should keep confidential any personal data, classified information, secrets protected by law and secrets obtained in the course of professional activities.</p> <p>Confidential information includes any data, fact or circumstance that an employer, data controller or data processor is not required by law to make available to the public during the term of their employment and after the termination thereof.</p>
Are there additional obligations, conditions, or exemptions in connection with the transfer of data to a third country or an international organisation?		
Art. 49(1) Art. 49(5)	Art. 13 (2)	International data transfers may be carried out under international agreements specified in Art. 96 GDPR (and Art. 61 of Directive 2016/680/EU) even in the absence of the conditions set out in the DPA.
Are there additional limits on the transfer of specific categories of personal data to a third country or an international organisation?		
Art. 49(5)	N/A	No
In a nutshell, what are the local regulations in connection with the supervisory authority's powers, due process and remedies against actions and decisions of the local supervisory authority?		
Art. 58 Art. 83(8)	Chapter V and VI (Sections 38 -61)	<p>The NAIH is an autonomous administrative agency and the central administrative body for the protection of personal data.</p> <p>It conducts inquiries, administrative proceedings and conducts data processing authorization procedures. It can act upon notification and ex officio.</p> <p>Furthermore, the NAIH enforces subjects to abide by the regulation and imposes fines and conducts certification procedures in line with Art. 42 GDPR.</p> <p>The NAIH publishes a report on its activities each year and presents this report to the Parliament. It makes recommendations for new regulations and for the amendment of legislations pertaining to the processing of personal data, to public information and information of public interests, and expresses its opinion on bills covering the same subject.</p>
Does a body, organisation or association have the right to: (i) lodge a complaint with the supervisory authority, (ii) sue for damages? Does this apply independently of a data subject's mandate, too? If so, which are these?		
Art. 80(2)	N/A	Yes, but only on the data subject's instructions.
Are there modifications regarding sanctions (including criminal offences) for breach? Please explain, including amount of fines or imprisonment, etc.		
Art. 84	Section 23	Data subjects are entitled to challenge the actions and acts of the data controller/processor directly before the courts. The burden of proof to ascertain that data processing is in compliance with the provisions of law or binding legislation of the European Union lies with the data controller and/or the data processor.

GDPR	DPA	HUNGARIAN IMPLEMENTATION
		<p>In its resolution adopted in administrative proceedings for data protection, the NAIH could apply the legal consequences provided for in the GDPR.</p> <p>The amount of administrative penalty if imposed upon a budgetary agency under Art. 83(7) GDPR is limited to an amount between HUF 100,000 and HUF 20 million (approx. EUR 60,000).</p>
Are there provisions to balance the protection of personal data with the rights to freedom of expression and information, including processing for journalistic, academic, artistic, or literary purposes?		
Art. 85	N/A	No
Are there specific rules regarding data processing relating to employment?		
Art. 88	N/A	No, the DPA does not introduce more specific requirements. These can be found in special laws (e.g. the Labour Code sets out a new legal bases for processing certain criminal and biometrical data of the employees).
Are there specific rules regarding the processing of personal data for scientific or historic research, statistical purposes, big data operations, etc?		
Art. 89	Section 5 (8)	The DPA allows bodies or persons conducting scientific research to disclose personal data if it is necessary to demonstrate the findings of the research in connection with historical events.
Any other relevant local law derogations to consider? (e.g. CCTV / video surveillance, provisions concerning the admissibility of processing of national identification numbers)		
Art. 87	N/A	The Execution Act made significant changes in numerous sectorial laws to deregulate in compliant sectorial provisions. For example, the strict retention periods regarding video surveillance records were abolished in the Act on Security Services and the Activities of Private Investigators, while the rules regarding granting explicit consent in relation to health data meets the requirements of the GDPR.
Are there any landmark decisions, material fines (including the underlying violation, eg violation of consent requirements), sector-focused investigations (e.g. banks, telecoms, health care) under the new law (GDPR or local DPA) to report so far?		
<p>In February 2019, the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) imposed the first significant sanction for violation of the GDPR in the amount of HUF 1,000,000 (approx. EUR 3,100). The sanction was imposed on company (data controller) for violating an individual's access rights to the company's CCTV system.</p> <p>The individual requested a copy of a CCTV record from the data controller which was required for him as evidence in a dispute. The company refused to provide the copy on the basis that the data subject failed to properly justify his legal claim to obtain the record. The NAIH stated that the data controller cannot request a justification in connection with the individual's request and in case of denying the request the individual should be informed of his further rights on the applicable remedies (right to turn to NAIH and/or courts).</p> <p>The imposed fine reached 6.5 % of the data controller's annual net sales revenue. NAIH considered the fact that the deleted CCTV record cannot be reinstated and the data was irrevocably lost when the fine was imposed.</p>		

This chapter was written by Janos Toth and Barnabas Buzasi.



JANOS TOTH
Partner

Wolf Theiss, Hungary

T. +36 1 4848 810
janos.toth@wolftheiss.com



BARNABAS BUZASI
Senior Associate

Wolf Theiss, Hungary

T. +36 1 4848 832
barnabas.buzasi@wolftheiss.com

POLAND

WOLF THEISS

NATIONAL IMPLEMENTING LEGISLATION IN A NUTSHELL

Poland incorporated the provisions of the GDPR by introducing the new Personal Data Protection Act (The Act of 10 May 2018 on the protection of personal data) and simultaneously the Provisions Implementing the Personal Data Protection Act (Act amending certain acts in connection with the application of the GDPR) – together as: “Implementing Law”.

The new Personal Data Protection Act extends GDPR requirements in some points. The Provisions Implementing the Personal Data Protection Act amended more than 160 sectoral acts, including banking, finance, insurance, administration, culture and labour acts, in order to adjust the sectoral regulations to the GDPR.

Here, we highlight the most important provisions of the Implementing Law which are within the framework of, but differ from, the GDPR. Outside of the scope of this Guide are provisions of the Implementing Law adopted for the purposes of transposing Directive (EU) 2016/680 into national legislation.

1. NATIONAL IMPLEMENTATION LAWS

1.1 Main Act

- 🔗 **The Act of 10 May 2018 on the protection of personal data**
Abb.: DPA
- 🔗 **Act amending certain acts in connection with the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC**
Abb.: IDPA

1.2 Other relevant law

- 🔗 **The Polish Act of 14 December 2018 on personal data protection regarding processing of personal data in connection with the prevention and combating of crime**
Abb.: APDC

1.3 Relevant ordinance / Other guideline

- 🔗 **Various industry codes have been created that specify how data are to be protected. One example is the health care sector, which describes how personal data contained within patients’ medical records may be shared in accordance with the GDPR.**

2. NATIONAL DATA PROTECTION AUTHORITY

- 🔗 **Polish Data Protection Authority / *Urząd Ochrony Danych Osobowych***
Abb.: UODO
English: <https://uodo.gov.pl/en>

3. NATIONAL IMPLEMENTATIONS / DEROGATIONS

GDPR	DPA /IDPA	POLISH IMPLEMENTATION
Apart from Art. 9 GDPR, are there any further conditions or limitations for processing special categories of personal data?		
Art. 9(2) a, b, j; Art. 9(4)	Art. 2 DPA Art. 14 APDC	The DPA excludes the application of the GDPR provisions prohibiting the processing of special categories of personal data for activities relating to the editing, preparation, creation or publication of press materials (as regulated by the Press Law Act) and literary or artistic activity. Under the APDC, special categories of personal data may be processed when: <ul style="list-style-type: none"> legislative provisions allow for their processing such processing is necessary to protect the life or health of the data subject or another person such data has been made public by the data subject concerned
Are there any additional authorisations required for processing personal data relating to criminal convictions/offences?		
Art. 10	Art. 1 APDC	The APDC authorizes the processing of personal data by competent authorities for the purposes of identifying, preventing, detecting and combating crimes (including threats to public safety), as well as applying punishment orders and coercive measures involving imprisonment.
Apart from Art. 13, 14 GDPR, are there any further obligations, conditions, or exemptions from information duties?		
Art. 13 Art. 14	Art. 2 APDC	The notification requirements under Art. 13 and 14 GDPR are excluded for journalistic, literary or artistic activity and the notification requirements under Art. 13 GDPR are excluded for academic statements. Under certain circumstances, there are also exemptions from information duties in the case of controllers carrying out public tasks.
Apart from the regulations under the GDPR, are there any further obligations, conditions, or exemptions from data subject rights?		
Art. 17(1) Art. 17(3) Art. 22(2) Art. 23 Art. 89(2) Art. 89(3)	Art. 2 DPA Art. 5 DPA Art. 11 IDPA Art. 6, 7, 16, 35, 81 IDPA	Some data subject rights do not apply in relation to journalistic, literary, or artistic activity and academic statements. The IDPA introduced a number of exemptions from data subjects' rights, in particular: <ul style="list-style-type: none"> The rights to rectification and restriction of processing are restricted with respect to the archiving activities of the state archive network. The right of access, restriction of data processing and the notification obligations regarding the rectification or erasure of personal data or restriction of data processing apply only to the extent that they do not infringe the confidentiality obligation of an attorney, attorney-at-law, notary in public, tax advisor, or sworn translator. The right to object to the processing of personal data does not apply in the case of data obtained by an attorney or attorney-at-law while providing legal advice, a notary in public while performing notarial acts, a tax advisor while rendering tax advice, or a sworn translator while translating.
Are there provisions that allow for the processing of data for secondary purposes (i.e. exceptions to the principle of purpose limitation in the case of a legal basis for processing)?		
Art. 6(4)	N/A	No
Is there any change to the age of consent for children?		
Art. 8	N/A	No
Are there additional obligations, conditions, or exemptions in connection with privacy impact assessments?		
Art. 35(10)	N/A	No
Are there any further obligations, conditions, or exemptions in connection with data processing by a processor?		
Art. 28(3) Art. 28(4) Art. 29 Art. 32(4)	N/A	No

GDPR	DPA /IDPA	POLISH IMPLEMENTATION
Are there any additional obligations when to appoint a data protection officer?		
Art. 37(4)	Art. 8 DPA Art. 10 DPA	No The appointment must be notified to the President of the UODO within 14 days from the date of appointment.
Are there additional obligations, conditions, or exemptions in connection with the transfer of data to a third country or an international organisation?		
Art. 49(1) Art. 49(5)	N/A	No
Are there additional limits on the transfer of specific categories of personal data to a third country or an international organisation?		
Art. 49(5)	N/A	No
In a nutshell, what are the local regulations in connection with the supervisory authority's powers, due process and remedies against actions and decisions of the local supervisory authority?		
Art. 58 Art. 83(8)	Chapters 6,7,9,11 DPA	The UODO is regulated by the DPA. The UODO is an administrative body charged with overseeing the protection of personal data, monitoring data processing and controlling compliance with data protections laws. In general, the UODO performs audits, requires subjects to abide by the regulation, informs the controllers and processors about their obligations and duties in the area of personal data protection, warns them about possible violations of the law, approves codes of conduct, deals with offences and imposes fines.
Does a body, organisation or association have the right to: (i) lodge a complaint with the supervisory authority, (ii) sue for damages? Does this apply independently of a data subject's mandate, too? If so, which are these?		
Art. 80(2)	Art. 61 DPA	A social organisation can represent a data subject on behalf of the data subject.
Are there modifications regarding sanctions (including criminal offences) for breach? Please explain, including amount of fines or imprisonment, etc.		
Art. 84	Chapter 11 DPA Chapter 9 ADPA	The DPA limits the maximum financial penalty for certain public entities to PLN 100,000 (approx. EUR 23,326). Under the ADPC, an individual who suffered damage or harm as a result of violation of provisions of the ADPC is entitled to damages or compensation from the data controller. In addition, anyone who hinders an inspection which is conducted to ensure compliance with personal data protection provisions is subject to a fine, restriction of personal liberty or imprisonment of up to two years. Finally, anyone who processes personal data without a valid legal basis is subject to a fine, restriction of personal liberty or imprisonment for up to two years (three years in case of sensitive data).
Are there provisions to balance the protection of personal data with the rights to freedom of expression and information, including processing for journalistic, academic, artistic, or literary purposes?		
Art. 85	Art. 2 DPA	A number of personal data protection rights have been excluded in the case of journalistic, literary or artistic activity, and academic statements. For instance: <ul style="list-style-type: none"> Information requirements where personal data are collected from data subjects Requirements to provide and obtain a copy of personal data undergoing processing Right to restriction of data processing Obligation to obtain records of processing activities etc.
Are there specific rules regarding data processing relating to employment?		
Art. 88	N/A	No, DPA does not introduce more specific employment-related provisions. Instead, the rules under employment law when processing employee data must be observed, e.g. restrictions on the data, which an employer can request from a job applicant/employee; collective labor agreement, work regulations in connection with CCTV or monitoring, consent requirements etc).

GDPR	DPA /IDPA	POLISH IMPLEMENTATION
Are there specific rules regarding the processing of personal data for scientific or historic research, statistical purposes, big data operations, etc?		
Art. 89	N/A	No Besides limiting the application of certain GDPR provisions to processing of personal data for the purposes of scientific or historical research, as well as to processing for statistical purposes, the Implementing Law does not introduce more specific provisions in this respect.
Any other relevant local law derogations to consider? (e.g. CCTV / video surveillance, provisions concerning the admissibility of processing of national identification numbers)		
Art. 87	IDPA	Data controllers, data processors, and their employees must ensure the confidentiality of personal data entrusted to them or accessible by them solely due to their employment. Video recordings containing personal data are processed only for the purposes for which they were collected and stored for a period not exceeding 3 months from the date of recording, unless separate provisions provide otherwise.
Are there any landmark decisions, material fines (including the underlying violation, eg violation of consent requirements), sector-focused investigations (e.g. banks, telecoms, health care) under the new law (GDPR or local DPA) to report so far?		
The UODO issued the first decision imposing an administrative fine in the amount of PLN 943,000 (approx. EUR 220,000) for the infringement of the information obligation stipulated in Art. 14 GDPR: A company processed data from publicly available registers informing only approx. 680,000 individuals of which it had the email address. The remaining over 6m data subjects were not informed even though their postal addresses were partially known. The company claimed the exemption from the information duty due to disproportional effort (Art. 14(5)b GDPR). The authority denied the application of the exemption in this case and the company announced it will appeal against the decision.		

This chapter was written by Peter Daszkowski, Agnieszka Nowak-Blaszczyk and Monika Gaczowska.



PETER DASZKOWSKI
Partner

Wolf Theiss, Poland

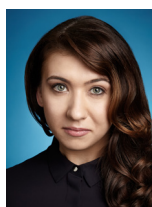
T. +48 22 3788 918
peter.daszkowski@wolftheiss.com



AGNIESZKA NOWAK-BLASCZYK
Senior Associate

Wolf Theiss, Poland

T. +48 22 3788 943
agnieszka.nowak-blaszczyk@wolftheiss.com



MONIKA GACZKOWSKA
Senior Associate

Wolf Theiss, Poland

T. +48 22 3788 957
monika.gaczowska@wolftheiss.com

WOLF THEISS

ROMANIA

NATIONAL IMPLEMENTING LEGISLATION IN A NUTSHELL

On 31 July 2018, Law no. 190/2018 on the measures for the application of the GDPR entered into force.

Law no. 190/2018 brings in some more rules on processing special categories of data, as well as some exemptions from the GDPR rules in case of certain categories of data processing. This law establishes the measures necessary for the national implementation of the provisions of, *inter alia*, Art. 6(2), Art. 9(4), Art. 37-39, 42, 43, Art. 83(7), Art. 85 and Art. 87-89 GDPR.

1. NATIONAL IMPLEMENTATION LAW

1.1 Main Act

- ⌘ Law no. 190/2018 on the measures for the application of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)
Abb.: Law 190/2018

1.2 Other relevant laws

- ⌘ Law no.102/2005 regarding the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing Law no. 129/2018 amending and supplementing Law no. 102/2005 regarding the setting up, organisation and functioning of the National Supervisory Authority for Personal Data Processing
- ⌘ Law no.506/2004 on the processing of personal data and the protection of privacy in the electronic communications sector
- ⌘ Law no. 682/2001 on the ratification of the Convention on the protection of individuals with regard to automatic processing of personal data, adopted in Strasbourg on 28 January 1981
- ⌘ Law no. 363/2018 on the protection of individuals with regard to the processing of personal data by competent authorities for the purpose of prevention, detection, investigation, criminal investigation and combating offences or the execution of sanctions, educational and safety measures, and on the free movement of such data¹

1.3 Relevant ordinances / Other guidelines

- ⌘ Decision of the National Supervisory Authority for Personal Data Processing no. 174/18.10.2018 regarding the list of operations for which the impact assessment on the protection of personal data is mandatory ("Black List")
- ⌘ Decision of the National Supervisory Authority for Personal Data Processing no. 161/09.10.2018 regarding the approval of the procedure of performing the investigations

¹ The analysis of this law does not fall within the scope of this guide.

2. NATIONAL DATA PROTECTION AUTHORITY

🔗 **The National Authority for the Supervision of Personal Data Processing / Romanian Data Protection Authority**

Abb.: NASDPD / RDPA

3. NATIONAL IMPLEMENTATIONS / DEROGATIONS

GDPR	LAW 190/2018	ROMANIAN IMPLEMENTATION
Apart from Art 9 GDPR, are there any further conditions or limitations for processing special categories of personal data?		
Art. 9(2) a, b, j; Art. 9(4)	Art.3 para 1 Art.6 Art.9 para 2	<p>Yes</p> <p>The processing of genetic, biometric or health-related data is allowed for the purpose of achieving an automated decision-making process or creating profiles when the data subject explicitly consents to it or, if the processing is based on express legal provisions, with the application of appropriate measures for the protection of the rights, freedoms and legitimate interests of the data subject.</p> <p>The processing of special categories of personal data in the context of carrying out a task in the public interest can also be performed provided that the controller/third party has instituted certain safeguards, such as: ensuring the security of personal data, designation of a data protection officer and establishing retention periods.</p> <p>Political parties and organisations of citizens belonging to national minorities and non-governmental organisations can also process special categories of personal data for the purposes of achieving their objectives, without the express consent of the data subject, on the condition that corresponding safeguards are provided (e.g. information of the data subject as regards the personal data processing, safeguarding the transparency of information, communication and means of exercising the rights of the data subject, safeguarding the right to rectification and deletion).</p>
Are there any additional authorisations required for processing personal data relating to criminal convictions/offences?		
Art. 10	N/A	<p>No</p> <p>The law does not provide for any such clause. However, according to the provisions of special laws, the employer may require criminal records from its employees holding certain positions (such as custodians).</p>
Apart from Art. 13, 14 GDPR, are there any further obligations, conditions, or exemptions from information duties?		
Art. 13 Art. 14	Art. 7 Art.15	<p>Yes</p> <p>The personal data processing for journalistic purposes or for academic, artistic or literary expression may be performed by derogation from certain provisions of the GDPR, including Art. 13 and 14.</p>
Apart from the regulations under the GDPR, are there any further obligations, conditions, or exemptions from data subject rights?		
Art. 17(1) Art. 17(3) Art. 22(2) Art. 23 Art. 89(2) Art. 89(3)	Art.7 Art. 8	<p>Yes</p> <p>The personal data processing for journalistic purposes or for academic, artistic or literary expression may be performed by derogation from Chapter III GDPR – Rights of the data subject.</p> <p>Also, the provisions of Art. 15, 16, 18 and 21 GDPR do not apply if personal data are processed for scientific or historical research purposes, statistic purposes or public interest archiving purposes, in so far as such rights mentioned in these articles, by their nature, render impossible or seriously impair the achievement of the specific purposes and those derogations are required for the fulfilment of these purposes.</p>

GDPR	LAW 190/2018	ROMANIAN IMPLEMENTATION
Are there provisions that allow for the processing of data for secondary purposes (i.e. exceptions to the principle of purpose limitation in the case of a legal basis for processing)?		
Art. 6(4)	Art.8	<p>Yes</p> <p>The law allows for processing for secondary purposes, such as, for scientific or historical research purposes, statistic purposes or public interest archiving purposes. In these cases, the data controller has to apply appropriate safeguards to protect the rights and freedoms of the data subjects, provided under Art. 89(1) GDPR.</p>
Is there any change to the age of consent for children?		
Art. 8	N/A	<p>No</p> <p>The law does not provide for specific regulations regarding the age of consent in the context of Art. 8 GDPR. Nonetheless, the Romanian Civil Code establishes that children may perform judicial acts of small value or administration actions starting at the age of 16. The assistance of the child's legal representative is required in case of judicial acts of higher values.</p> <p>Therefore, the age of consent is 16 for the purpose of personal data processing in relation to information society services.</p>
Are there additional obligations, conditions, or exemptions in connection with privacy impact assessments?		
Art. 35(10)	N/A	<p>No</p> <p>See only Romanian Black-List (link above).</p>
Are there any further obligations, conditions, or exemptions in connection with data processing by a processor?		
Art. 28(3) Art. 28(4) Art. 29 Art. 32(4)	N/A	No
Are there any further additional obligations when to appoint a data protection officer?		
Art. 37(4)	Art. 4 para 2, letter b) Art. 6, letter b)	<p>Yes</p> <p>Additionally it is also necessary to appoint a data protection officer:</p> <ul style="list-style-type: none"> for the processing of a national identification number; for the processing personal data and special categories of personal data in the context of carrying out a task in public interest.
Are there additional obligations, conditions, or exemptions in connection with the transfer of data to a third country or an international organisation?		
Art. 49(1) Art. 49(5)	N/A	No
Are there additional limits on the transfer of specific categories of personal data to a third country or an international organisation?		
Art. 49(5)	N/A	No
In a nutshell, what are the local regulations in connection with the supervisory authority's powers, due process and remedies against actions and decisions of the local supervisory authority?		
Art. 58 Art. 83(8)	Law 102/2005 Law 129/2018 RDPA Decision 161/ 2018	The RDPA carries out its activities independently and impartially. It supervises and controls the legality of personal data processing which falls under the Law 190/2018 and the GDPR. For this purpose, the RDPA has specific prerogatives, such as:

GDPR	LAW 190/2018	ROMANIAN IMPLEMENTATION
		<p>i.) It informs the controllers and processors about their obligations and duties in the area of personal data protection.</p> <p>ii.) It approves codes of conduct, receives and solves the complaints/request of the data subjects and communicates the given solution or, according to each case, the approaches carried out.</p> <p>iii.) It performs investigations, deals with offences and imposes fines.</p> <p>iv.) It provides consulting in the area of personal data protection.</p> <p>v.) Law no. 102/2005 was completed by Law no. 129/2018 with new chapters, detailing the control duties and procedures for resolving complaints by the authority and also the relevant judicial remedies available in relation to data subjects and controllers/processors.</p> <p>vi.) The control personnel of the RDPA are now entitled to carry out investigations (including unannounced ones) and to request and obtain any information and documents (regardless of the storage support) from the data controller/processor or their representatives.</p> <p>vii.) Fines of up to EUR 300,000 may be imposed by the inspectors of the RDPA through the minutes concluded on the field. Higher fines may also be imposed on the Decision of the RDPA President.</p>
<p>Does a body, organisation or association have the right to: (i) lodge a complaint with the supervisory authority, (ii) sue for damages? Does this apply independently of a data subject's mandate, too? If so, which are these?</p>		
Art. 80(2)	N/A	No
<p>Are there modifications regarding sanctions (including criminal offences) for breach? Please explain, including amount of fines or imprisonment, etc.</p>		
Art. 84	Art. 14 para 4 and 6	<p>Yes</p> <p>The law imposes significantly lower penalties or sanctions on public authorities compared to companies.</p> <p>The RDPA cannot apply fines higher than RON 200,000 (EUR 42,000 approximately) on public authorities/institutions, religious units and non-governmental organisations acting in the public interest, for failing to comply with the GDPR's provisions or for failing to implement remediation plans drafted by the RDPA.</p> <p>Furthermore, the possibility to eliminate any data protection breaches within a grace period of up to three months, based on a predetermined resolution plan is only provided for public authorities/institutions, religious units and non-governmental organisations acting in public interest.</p>
<p>Are there provisions to balance the protection of personal data with the rights to freedom of expression and information, including processing for journalistic, academic, artistic, or literary purposes?</p>		
Art. 85	Art. 7	<p>Yes</p> <p>To ensure a balance between the right to personal data protection, the freedom of expression and the right to information, data processing for journalistic purposes or for academic, artistic or literary expression may be carried out, provided that it refers to personal data that was expressly made public by the data subject or which is strictly related to the quality of the public person of the data subject or the public character of the facts that the person is involved in.</p>
<p>Are there specific rules regarding data processing relating to employment?</p>		
Art. 88	Art. 5	<p>Yes</p> <p>The law provides for specific rules regarding the processing of data relating to employment. In cases where workplace monitoring systems through electronic communications and/or video surveillance measures are used, the processing of personal data being performed is based on the legitimate interest of the employer.</p>

GDPR	LAW 190/2018	ROMANIAN IMPLEMENTATION
		<p>Prior to implementing any monitoring measures in the workplace, the employer must make sure that other less intrusive methods have been tested and have not proven to be efficient. This means an actual and documented attempt from the employer. Also, employees' representatives or the trade union must be consulted.</p> <p>The duration for which personal data may be stored cannot exceed 30 days (unless other legal grounds are applicable). The extension of the period should be documented in advance.</p>
Are there specific rules regarding the processing of personal data for scientific or historic research, statistical purposes, big data operations, etc.?		
Art. 89	N/A	No
Any other relevant local law derogations to consider? (e.g. CCTV / video surveillance, provisions concerning the admissibility of processing of national identification numbers)		
Art. 87	N/A	No
Are there any landmark decisions, material fines (including the underlying violation, eg violation of consent requirements), sector-focused investigations (e.g. banks, telecoms, health care) under the new law (GDPR or local DPA) to report so far?		
No		

This chapter was written by Maria Maxim and Nina Lazar.



MARIA MAXIM
Partner

Wolf Theiss, Romania

T. +40 21 3088 104
maria.maxim@wolftheiss.com



NINA LAZAR
Associate

Wolf Theiss, Romania

T. +40 21 3088 184
nina.lazar@wolftheiss.com

SLOVAK REPUBLIC

NATIONAL IMPLEMENTING LEGISLATION IN A NUTSHELL

The Slovak data protection law is governed by the Act No. 18/2018 Coll. on Protection of Personal Data (*zákon o ochrane osobných údajov*) (the “**Data Protection Act**” or “**DPA**”) which entered into force on 25 May 2018 implementing the GDPR and repealed the Act No. 122/2013 Coll. on Personal Data Protection, as amended.

1. NATIONAL IMPLEMENTATION LAWS

1.1 Main Act

- ⌘ **Data Protection Act / Zákon o ochrane osobných údajov**
Abb.: DPA

1.2 Other relevant law

- ⌘ **The Decree of the Office for Personal Data Protection no. 158/2018 Coll. on Data Protection Impact Assessment Procedure / Vyhláška Úradu na ochranu osobných údajov SR č. 158/2018 Z. z. o postupe pri posudzovaní vplyvu na ochranu osobných údajov**
Abb.: Decree

1.3 Relevant ordinances / Other guidelines

- ⌘ **List of processing operations subject to impact assessment / Zoznam spracovateľských operácií, ktoré podliehajú posúdeniu vplyvu (so-called Black List)**
- ⌘ **Legal processing of personal data related to clinical testing / Záonné spracúvanie osobných údajov pri klinickom skúšaní**
- ⌘ **Methodology compliance of personal data processing at schools / Metodika súladu spracúvania osobných údajov v prostredí škôl**
- ⌘ **Guideline No. 2/2018 – legal basis of processing. Updated version as of 22 January 2019 / Metodické usmernenie č. 2/2018 – Záonnosť spracúvania. Aktualizovaná verzia zo dňa 22.01.2019**
- ⌘ **Frequently asked questions related to photography and audiovisual records / Často kladené otázky k fotografiám a audiovizuálnym záznam**
- ⌘ **Statement of the Data Protection Office of the Slovak Republic related to delivery writings in an administrative proceeding and administrative file inspection / Stanovisko ÚOOÚ SR k doručovaniu písomností v správnom konaní a nazeranie do administratívneho spisu**
- ⌘ **Natural persons – entrepreneurs and legal persons standing from the data protection perspective / Postavenie právnických osôb a fyzických osôb – podnikateľov z pohľadu ochrany osobných údajov**
- ⌘ **Guideline No. 3/2018 – e-shop controller duties / MU č. 3_2018 k povinnostiam prevádzkovateľa e-shopu**
- ⌘ **Guideline No. 2/2018 – legal basis of processing / MU č. 2_2018 k záonnosti spracúvania**

- ⌘ Terms “Fundamental rights and freedoms” versus “rights and freedoms” – how to define them / *Pojmy “Základné práva a slobody” verzus “práva a slobody” – a ako ich identifikovať*
- ⌘ Administrator of the social network fanpage as a controller / *Správca fanúšikovskej stránky umiestnenej na sociálnej sieti v postavení prevádzkovateľa*
- ⌘ Guideline – when the regulation and when the act on data protection? / *Metodika – Kedy nariadenie a kedy zákon o ochrane osobných údajov?*
- ⌘ Designation / *K oznamovaniu určenia zodpovednej osoby a jej kontaktných údajov úradu podľa novej právnej úpravy*
- ⌘ Authorised person and instruction of authorised person under new legislation / *Oprávnená osoba a poučenie oprávnenej osoby podľa novej právnej úpravy*
- ⌘ 30 steps of the compliance with the new legislation on personal data protection / *30 krokov súladu s novou právnou úpravou ochrany osobných údajov*
- ⌘ Guidelines for cities and municipalities / *Metodiky pre mestá a obce*

2. NATIONAL DATA PROTECTION AUTHORITY

- ⌘ Data Protection Office of the Slovak Republic / *Úrad na ochranu osobných údajov Slovenskej republiky*
Abb.: DPO

3. NATIONAL IMPLEMENTATIONS / DEROGATIONS

GDPR	DPA	SLOVAK IMPLEMENTATION
Apart from Art. 9 GDPR, are there any further conditions or limitations for processing special categories of personal data?		
Art. 9(2) a, b, j; Art. 9(4)	§ 16	<p>Yes, there is an additional requirement. The consent to process sensitive data is void if granting such consent is excluded by a separate regulation.</p> <p>Processing is also permitted when;</p> <ul style="list-style-type: none"> ▪ It is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or the data subject in the area of labour law, social law insurance, social protection, or public health insurance; and ▪ it is necessary for the purpose of social insurance, social security for police and soldiers, and providing specific social benefits.
Are there any additional authorisations required for processing personal data relating to criminal convictions/offences?		
Art. 10	§ 17	<ul style="list-style-type: none"> ▪ Under the DPA only a state body may be a data controller for personal data relating to criminal convictions/offences. ▪ As regards criminal record background checks in an employment context, no official opinion has been issued on this matter by the DPO.
Apart from Art 13, 14 GDPR, are there any further obligations, conditions, or exemptions from information duties?		
Art. 13	§ 19	No
Art. 14	§ 20	

GDPR	DPA	SLOVAK IMPLEMENTATION
Apart from the regulations under the GDPR, are there any further obligations, conditions, or exemptions from data subject rights?		
Art. 17(1) Art. 17(3) Art. 22(2) Art. 23 Art. 89(2) Art. 89(3)	§ 23-25 § 28(2) § 30 § 78(9) § 78(10)	Rights and obligations stated in the GDPR correspond with the provisions of the DPA. However, an additional condition is that data subjects rights may be restricted on grounds of Slovak public policy or economic mobilization.
Are there provisions that allow for the processing of data for secondary purposes (i.e. exceptions to the principle of purpose limitation in the case of a legal basis for processing)?		
Art. 6(4)	§ 13(3)	Conditions allowing for processing for secondary purposes in the DPA are the same as those provided in the GDPR.
Is there any change to the age of consent for children?		
Art 8	§ 15	No
Are there additional obligations, conditions, or exemptions in connection with privacy impact assessments?		
Art. 35(10)	N/A	No
Are there any further obligations, conditions, or exemptions in connection with data processing by a processor?		
Art. 28(3) Art. 28(4) Art. 29 Art. 32(4)	§ 34 § 36 § 39(4)	No The rights and obligations stated in the GDPR correspond with the provisions of the DPA.
Are there any additional obligations when to appoint a data protection officer?		
Art. 37(4)	§ 44(5)	No
Are there additional obligations, conditions, or exemptions in connection with the transfer of data to a third country or an international organisation?		
Art. 49(1) Art. 49(5)	§ 51(1), (2)	No
Are there additional limits on the transfer of specific categories of personal data to a third country or an international organisation?		
Art. 49(5)	N/A	No
In a nutshell, what are the local regulations in connection with the supervisory authority's powers, due process and remedies against actions and decisions of the local supervisory authority?		
Art. 58 Art. 83(8)	§ 80 § 99-103 § 104-106	Rights and obligations stated in the GDPR correspond with the provisions of the DPA. Additionally, the DPO is authorized to invite the controller or processor to submit an explanation of suspected breaches of the DPA, special regulation, or international law. The DPO's scope of competence does not include contractual disputes between the controller/processor and another person if the court and other bodies are competent to hear and decide the dispute. The DPO may also charge an appropriate fee for administrative costs or refuse to act on an application if it is manifestly unfounded, inappropriate, or repetitive. As regards the administrative sanctions, the DPA empowers the DPO to impose a fine of up to EUR 2,000 on persons who are not the controller or processor for failure to cooperate with the DPO. The DPO may also fine the controller or processor if it fails to ensure adequate conditions for the exercise of DPO controls under the DPA.

GDPR	DPA	SLOVAK IMPLEMENTATION
Does a body, organisation or association have the right to: (i) lodge a complaint with the supervisory authority, (ii) sue for damages? Does this apply independently of a data subject's mandate, too? If so, which are these?		
Art. 80(2)	N/A	Yes, but only on the data subject's instructions.
Are there modifications regarding sanctions (including criminal offences) for breach? Please explain, including amount of fines or imprisonment, etc.		
Art. 84	§ 104	No The DPA recognizes only financial sanctions, however the Criminal Code sets out a criminal offence for the unlawful processing of personal data which was obtained under an obligation of confidentiality (punishable with up to 2 years of imprisonment).
Are there provisions to balance the protection of personal data with the rights to freedom of expression and information, including processing for journalistic, academic, artistic, or literary purposes?		
Art. 85	§ 78(1)	Under the DPA, the data controller is entitled to process personal data without the consent of the data subject, if the processing is necessary for academic, artistic or literary purposes.
Are there specific rules regarding data processing relating to employment?		
Art. 88	§ 78(3)	The employer may provide or publish personal data such as the title, name, surname, job, service or administrative position, department, place of work, telephone number, fax number or electronic address of workplace and identification data of the employee if it is necessary for the fulfilment of the job, service or administrative duties of the data subject. However, publishing such personal data cannot violate the respect, dignity and safety of the data subject.
Are there specific rules regarding the processing of personal data for scientific or historic research, statistical purposes, big data operations, etc?		
Art. 89	§ 78	No
Any other relevant local law derogations to consider? (e.g. CCTV / video surveillance, provisions concerning the admissibility of processing of national identification numbers)		
Art. 87	N/A	There are no derogations.
Are there any landmark decisions, material fines (including the underlying violation, eg violation of consent requirements), sector-focused investigations (e.g. banks, telecoms, health care) under the new law (GDPR or local DPA) to report so far?		
So far, we are not aware of any fines or cases in this regard.		

This chapter was written by Katarína Bielíková and Dalibor Palatický.



KATARÍNA BIELÍKOVÁ
Counsel

Wolf Theiss, Slovak Republic

T. +421 2 591 012 50
katarina.bielikova@wolftheiss.com



DALIBOR PALATICKÝ
Associate

Wolf Theiss, Slovak Republic

T. +421 2 591 012 47
dalibor.palaticky@wolftheiss.com

WOLF THEISS

SLOVENIA

NATIONAL IMPLEMENTING LEGISLATION IN A NUTSHELL

Still to be implemented.

OUR OFFICES

ALBANIA

Murat Toptani Street
AL - 1001 Tirana
T. +355 4 227 45 21
E. tirana@wolftheiss.com

AUSTRIA

Schubertring 6
A - 1010 Vienna
T. +43 1 515 10
E. wien@wolftheiss.com

BOSNIA AND HERZEGOVINA

Zmaja od Bosne 7
BiH - 71 000 Sarajevo
T. + 387 33 953 444
E. sarajevo@wolftheiss.com

BULGARIA

55 Nikola Vaptsarov Blvd.
BG - 1407 Sofia
T. +359 2 861 37 00
E. sofia@wolftheiss.com

CROATIA

Ivana Lučića 2a/19
HR - 10 000 Zagreb
T. +385 1 4925 400
E. zagreb@wolftheiss.com

CZECH REPUBLIC

Pobřežní 12
CZ - 186 00 Praha 8
T. +420 234 765 111
E. [praaha@wolftheiss.com](mailto:praha@wolftheiss.com)

HUNGARY

Kálvin tér 12-13
H - 1085 Budapest
T. +36 1 484 88 00
E. budapest@wolftheiss.com

POLAND

ul. Mokotowska 49
PL - 00-542 Warszawa
T. +48 22 3788 900
E. warszawa@wolftheiss.com

ROMANIA

4 Vasile Alecsandri Street
RO - 010639 Bucharest
T. +40 21 3088 100
E. bucuresti@wolftheiss.com

SERBIA

Bulevar Mihajla Pupina 6/18
SRB - 11000 Novi Beograd
T. +381 11 330 29 00
E. beograd@wolftheiss.com

SLOVAK REPUBLIC

Aupark Tower, Einsteinova 24
SK - 851 01 Bratislava
T. +421 2 591 012 40
E. bratislava@wolftheiss.com

SLOVENIA

Bleiweisova cesta 30
SI - 1000 Ljubljana
T. +386 1 438 00 00
E. [ljublana@wolftheiss.com](mailto:ljubljana@wolftheiss.com)

UKRAINE

9A, Khoryva Street
UA - 04071 Kyiv
T. +380 44 3777 500
E. kiev@wolftheiss.com

WOLF THEISS is one of the largest and most respected law firms in Central, Eastern and Southeastern Europe (CEE/SEE). We opened our first office in Vienna over 60 years ago. Our team now brings together over 340 lawyers from a diverse range of backgrounds, working in offices in 13 countries throughout the CEE/SEE region. During that time, we have worked on many cases that have broken new ground.

We concentrate our energies on a unique part of the world: the complex, fast-moving markets of the CEE/SEE region. This is a fascinating area, influenced by a variety of cultural, political and economic trends. We enjoy analysing and reflecting on those changes, drawing on our experiences, and working on a wide range of domestic and cross-border cases.