Deloitte.
Legal

Living one year with GDPR

Practitioner Perspectives

Contents

Introduction 4

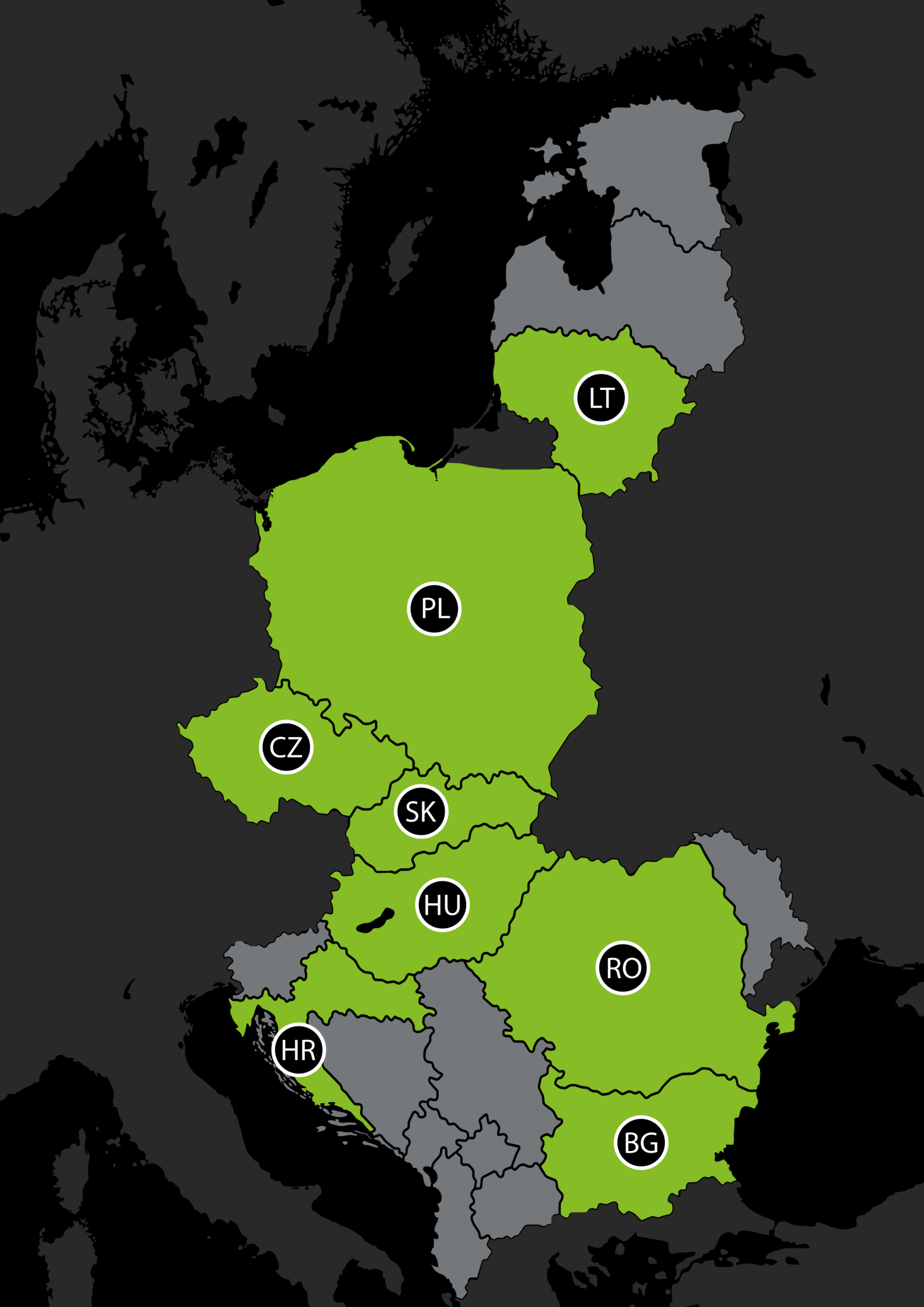
The controls and fines imposed by local Data Protection Authorities 5

Specific local provisions of law regarding personal data protection 9

Personal data violations reported to Data Protection Authorities 13

Summary 16

Contacts 17


LT
PL
CZ
SK
HU
RO
HR
BG

Introduction

The GDPR has been one of the most significant disruptions in terms of compliance regulations in recent memory. As it involves entities from all sectors, it has become an issue for every entity which processes personal data. The introduction and application of new provisions of law have created significant challenges for the market. After one year of the GDPR applicability, we have prepared this report providing key information about some of the most important issues when it comes to the application of the GDPR. It addresses the main changes in national laws in the area of personal data protection, provides for an overview of control and fines as well as focuses on the most notorious breaches of personal data protection rules. We hope you will find this report interesting and useful.

Best regards,
Deloitte Legal Central Europe GDPR team

The controls and fines imposed by local Data Protection Authorities

Bulgaria

The Bulgarian supervisory authority, which is the Commission for Personal Data Protect (CPDP), has published a report for its activity in 2018, according to which the complaints during the year were over 780. A large increase of complaints was observed after 25 May 2018. They were mainly related to personal data processing without legal grounds, and insufficient technical and organizational measures taken by controllers. Most of the submitted complaints were against controllers from the telecom and banking sector, as well as public sector and media. The number of sanctions imposed during 2018 was 13, which amount to BGN 246 500.00 (EUR 123,250.00).

An interesting case is about a Bulgarian bank that has been fined BGN 1,000 (EUR 511) by the CPDP for failing to comply with the "purpose limitation" principle under the GDPR. Personal data has been collected with respect to a credit agreement with the data subject and further processed by the bank in an incompatible manner. The CPDP has also exercised its corrective powers by imposing a definitive limitation on data processing until expiration of the retention period, since there is no longer a relationship between the data subject and the bank.

The biggest fine so far (BGN 53 000, approx. EUR 27,000) has been imposed on a telecom for processing personal data without legal grounds. It has repeatedly registered prepaid services without the knowledge and consent of the data subject. Circumstances considered by the CPDP when imposing a fine were that other corrective measures are not appropriate, and that fines have been imposed on the telecom several times before, including for a similar violation.

Generally, sanctions by the CPDP could be challenged before the court. There is no publicly available information whether this has been done with respect to the cases mentioned above.

For now, the CPDP has not published a plan of controls for specific sectors, nor information what will they be taking into account.

The Czech Republic

To date, **eight fines** based on the GDPR were imposed by **the Office for Personal Data Protection** (ÚOOÚ). Six of them are already effective and enforceable, they amounted to the sums **from approximately EUR 390 to EUR 1.170** and were results of failure to provide requested information contrary to the right of access by the data subject (two cases), inappropriate data security (two cases), data processing without necessary consent (one case), breach of the principle of lawful, fair and transparent data processing (one case). There are two fines imposed but not effective yet, sanctioning data processing without necessary consent (cca EUR 1.945) and breach of the principles of data minimisation and storage limitation (cca EUR 9.730)

ÚOOÚ has presented its **plan of controls** for 2019 stating it will focus on meeting the obligations primarily at the medical facilities and at the companies developing or engaging mobile applications. The plan also mentions issues like cookies, e-government, political parties, online loan agreements, transportation tickets, DNA tests or fingerprints in connection with gambling.

Slovakia

We are not aware of any major fines imposed, so far. However, pursuant to the unofficial information, the controls should intensify in the coming months. According to the published plan of controls, the Data Protection Authority should focus primarily on public institutions, companies using biometrics and providing postal services, etc.

According to the published plan of controls, national data protection authority should focus on consistency of the processing of the personal data of the persons concerned with the principles of the processing of personal data. It should also take into consideration the conditions of legal processing and the restrictions on the processing of specific categories of personal data together with the data subjects' rights and personal data security.

Lithuania

Recently, the State Data Protection Inspectorate has imposed its first fine in the amount of €61,500 on a FinTech company MisterTango, UAB. The fine was imposed for inappropriate data processing, disclosing of personal data and failing to provide notification on data breach to the supervisory authority.

According to the State Data Protection Inspectorate, MisterTango suffered a data breach in July 2018, when its customers' personal information in more than 9,000 screenshots of banking transactions became available online. The company decided not to notify the State Data Protection Inspectorate about the data breach occurred and in such way violated Article 33 of the GDPR.

Poland

On 15 March 2019, the President of the Personal Data Protection Office imposed the first financial penalty for breach of the GDPR. The penalty concerned failure to provide data subjects with information about the processing of their data by the controller. The company in question processed data of persons obtained from publicly available sources, including from the Central Register and Information on Business (CEiDG), and processed them for profit. The controller fulfilled the information obligation, providing information required by art. 14 par. 1-3 GDPR only to those persons to whom he had e-mail addresses. In the case of other people, he did not due to the high costs of such an operation. That is why only an information clause was posted on his website. The authority not only requested to remove the detected irregularities through presenting relevant information. It also imposed a financial penalty in the amount of PLN 943,470.00.

Another financial penalty was imposed on 25 April 2019, the main reason for the imposition of the penalty on the controller

were ineffective attempts to remove the violation consisted of the publicizing of a too wide range of personal data. The Dolnośląski Football Association made public the personal data of the judges who were granted the judges' licenses, not only their names and surnames were public, but also their exact residence addresses and PESEL numbers. By setting the fine - PLN 55 750.50, account was taken of duration of the infringement and the fact that it concerned a large group of persons (585). It was decided that although the violation was finally remediated, it was serious. The mitigating circumstances were also taken into account, including good cooperation between the controller and the supervisory body and lack of evidence that damage occurred to persons whose data was disclosed.

According to the yearly sector control plan, in 2019 the Personal Data Protection Office will verify the processing of personal data in areas such as: telemarketing, profiling in the banking and insurance sector or the waste identification and monitoring system. It will be also checked whether disclosure of data in the Public Information Bulletin by entities obliged to do so does not violate the provisions on the protection of personal data. In 2019, a closer look will be taken at such entities as: police, border guard and detention centers, by checking their use of technical and organizational measures aimed at preventing unauthorized access, copying, changing or deleting data. Scheduled inspections are dictated mainly by numerous signals (including complaints, questions and reports of violations of personal data protection) indicating the threat of violation of the provisions on the protection of personal data in the abovementioned areas.

Romania

Based on information made public by the Romanian Data Protection Authority, it appears that after the entry into force of the GDPR and until 24th of May 2019, the authority initiated 485 ex oficio controls, and 496 controls based on prior complaints of individuals. As a result, the Romanian Data Protection Authority did not impose fines, however, it imposed 57 corrective measures and 23 warnings in this respect.

Furthermore, based on our practical experience with the Romanian Data Protection Authority, it has performed controls with respect to the data processing activities pertaining to the implementation of CCTV systems, sending of direct marketing messages, non-observance of data subjects' rights' , and compliance with the data protection principles (e.g., data retention, purpose limitation etc.), the Romanian Data Protection Authority has investigated the security measures implemented by controllers or processors in relation to data breaches that were notified.

The areas of interest for the Romanian Data Protection Authority will be controllers or processors operating in the electronic communications, banking and marketing sectors. The object of controls may, in particular, refer to:

- the qualification of controller or processor and the applicable organizational or technical security measures,
- the duties of the controller or processor (e.g. data protection by design, implementation of security measures, performance of DPIAs etc.), and
- the compliance with the data protection processing principles.

Hungary

In Hungary, we may list 9 to 10 cases closed by the Hungarian DPA since the GDPR became applicable. The fines imposed range between the amount of EUR 3000 and EUR 40.000. These cases included various aspects of infringements, such as failing to report data breach or to notify data subjects properly on such data breach, handing over personal data to third parties without proper legal basis, non-compliance in handling data subject requests, non-compliance with the right to erasure, the principle of accuracy and CCTV usage.

The case resulting in the maximum amount of fines included the infringement of Articles 33 and 34 for failing to report personal data breach and notify the data subjects accordingly. The user data base of a political party (data controller's website) containing the names, e-mail addresses and encrypted account passwords of the users, became accessible via the internet due to a hacker attack and the hacker made available information on the methods used on its website.

Croatia

There are no publicly available data about controls and fines imposed by Croatian Data Protection Authority i.e. Agencija za zaštitu podataka ("**AZOP**"). Additionally, based on the informal data we were provided with, **AZOP** has not imposed any fine so far.

So far, based on some informal data, **AZOP** has not initiated any investigation procedures. However, it is expected that the investigation procedures might be performed similar to the investigations that were performed in accordance with the Croatian Data Protection Act i.e. an act that was applicable before the GDPR entered into force. If that will be the case, **AZOP** will take the following steps in the investigations:

- send a questionnaire to the entity under investigation and based on the provided answers decide on taking further investigation actions;
- execute investigation actions e.g. IT inspection; review of data protection internal procedures, etc.;
- make a decision based on the investigation.


A1
INNOVATION
Data-A

Specific local provisions of law regarding personal data protection

Bulgaria

Apart from the above, the CPDP has already adopted a list of ten processing activities where data protection impact assessment (DPIA) is mandatory.

The amendments to the Bulgarian Personal Data Protection Act (PDPA) adopted in connection with the GDPR were promulgated in February 2019. Some of the most important changes concern processing of personal data by employers. They have to adopt rules and procedures in certain cases, among which restricting the use of internal resources (e.g. restrictions on Internet use by employees), or introducing access control systems, or systems for control of working time and labor discipline (e.g. GPS systems for tracking company cars). In addition, employers have to determine a retention period for processing personal data of job applicants, which can be no longer than 6 months, unless an applicant has given consent for a longer storage period.

Specific PDPA provisions regulate handling ID documents and PIN, processing personal data of children under 14 years of age based on consent, as well as of deceased persons' data, content of the request for exercising data subjects' rights, deadline for exercising rights before the supervisory authority, etc.

The PDPA contains special provisions regarding personal data processing when exercising the right to information and freedom of expression, including for journalistic purposes. The rules provoked a lively public debate a few months ago, and were vetoed by the Bulgarian President. In particular, the motion veto refers to the provision of ten different criteria for the processing of personal data for journalistic purposes. According to the President, this could lead to overregulation and a need for a continuous balancing of the right to protection of data with the right to freedom of expression and information. However, these considerations were not accepted by the Bulgarian Parliament and the Motion was overturned in February 2019.

The Czech Republic

On 24 April 2019, two new data protection acts, together referred to as "**the GDPR Adaptation Acts**", were published in the Czech Collection of Laws and thus became effective. The implementation consists of:

- **the Act No. 110/2019 Coll**., on Personal Data Processing ("PDP Act"), which will replace the existing Act No. 101/2000 Coll., on Personal Data Protection;
- **the accompanying Act No. 111/2019 Coll**., amending certain acts in connection with the adoption of the Act on Personal Data Processing ("Accompanying Act").

The PDP Act mostly specifies provisions already established by the GDPR, the national discretionary power enabled for by the GDPR was applied only to a limited extend by the Czech legislators. Clarification of data processing rules in the public sector prevails in the final text and it has no major impact on the private sector. The adaption of the PDP Act affects, for example, the following:

- **The Office for Personal Data Protection** (ÚOOÚ) remains the supervisory authority for the data protection matters in the Czech Republic.
- The possibility of imposing **administrative sanctions** for the personal data breach on **some public entities** (municipalities not having extended powers in the scope of the municipal authority of a municipality with extended powers, and educational facilities established by municipalities) is **fully abolished**.
- Certain exemptions from the obligation of the controller to carry out **the data protection impact assessment (DPIA)** in situations where data processing is ordered directly by law are allowed.
- Fulfilment of **the information obligation** in case of data processing based on legal obligation, for example towards employees, or in public interest, is sufficient using the means of **distant access (**intranet, internet).
- In order to secure a defined '**protected interest**' (e.g. national defence, prevention and detection of criminal offenses), some rights of data subjects as well as data breach notification obligation may be restricted. Moreover, due to the 'protected interest' an exemption to assess compatibility of further data processing with the initial purpose of data collection within the meaning of Art. 6 (4) GDPR applies.
- The processing of personal data for the purpose of **scientific or historical research**, or for **the statistical**, **journalistic**, **academic or artistic purposes** is regulated in more detail.
- The age limit for granting the consent to the processing of personal data for the purpose of providing information society services is set to **15 years** (i.e. decreased by one year compared to the GDPR).

Slovakia

Slovak Republic has adopted Law no. 18/2018 Coll. on Personal Data Protection ("Act on Data Protection") that to wide extend copies the GDPR. Act on Data Protection largely duplicates the provisions of the GDPR, however, there are also exceptions and derogations in GDPR context. These includes mainly specific possibilities to process personal data for selected purposes without the consent of the data subject. The employers are in certain cases entitled to publish contact details of the employee and there are also further specifications on processing and publication of birth numbers.

In addition to the above, some acts have been amended in the light of the new data protection legislation. Some of these amendments have brought certain complications in everyday practice of business and data subjects. For example, duplicity of legal basis for data processing has been introduced by the amendment to the Act No. 455/1991 Coll. on Trade Licensing, which requires consent, even in cases, where there is other legal basis primarily applicable.

Lithuania

The Law on Legal Protection of Personal Data establishes some peculiarities for data processing, specifically related to the processing of personal identification code and processing of personal data for the purpose of freedom of expression and information. The mentioned law also sets specific requirements applicable to personal data processing in the context of employment relations and establishes the age limit for a child to whom the information society service is offered.

Additionally, the State Data Protection Inspectorate adopted a list of activities that are subject to obligatory DPIA. Based on such list, telephone conversations recording; biometric and genetic data processing; processing of personal video and/or audio data in the workplace, at the controller's premises or in areas where employees are working; processing of personal data related to monitoring of employees, its communication, behaviour or movement and similar activities are subject to obligatory DPIA. However, according to the observed practises, most of the data controllers have not performed DPIA as required.

Poland

As of 4 May 2019, a sectoral law implementing the GDPR has come into force, the main task of which is to adapt almost 170 legal acts to the requirements of the EU regulation. The changes concern in particular the scope and manner of performing the information obligation and obtaining consent, profiling, or the manner of exercising the rights of data subjects, and it introduces specific provisions as the legal basis for data processing.

In the regard of labor law, an employer may request personal data when it is necessary to perform specific types of work or a specific position. The employer may process personal data of the applicant or employee, based on their consent, with the exception of information on convictions and violations of the law. In addition, the processing of special categories of data based on consent will be possible only when the transfer takes place at the initiative of the person applying for employment or an employee. Only persons who have a written authorization from the employer and are obliged to keep confidential may be allowed to process such specific personal data.

In banking and insurance law, additional rights for consumers were provided. At the request of the a natural person, legal entity or organizational unit without legal personality, as long as it has legal capacity, applying for a loan, the bank will present the factors, including personal data, which had an impact on the creditworthiness assessment. In the insurance and reinsurance activities, the basis for processing data on health was introduced. Pursuant to the amendment, the insurance company processes health data of the insured persons or persons authorized under the insurance contract or statements submitted before the conclusion of the insurance contract, respectively to assess the risk or perform the contract to the extent necessary by the purpose and type of insurance.

One of the most important duties imposed on entrepreneurs by the GDPR is that of providing the data subject with relevant information related to the processing of his personal data. The sectoral law provides the convenience for micro-entrepreneurs in the implementation of the information obligation. The micro-entrepreneurs perform this obligation by displaying relevant information in a noticeable place at the business premises or by making it available on its website. The indicated manner of fulfilling the information obligation is possible only in the case of obtaining personal data directly from the data subject.

Romania

Law no. 190/2018 complements the GDPR in Romania and includes additional/ derogatory provisions in the areas where the GDPR provided for such possibility.

Law 190/2018 includes, among others, provisions regarding the processing of personal identification numbers based on legitimate interest, which prior to the GDPR was not permitted. In this case,

the controller will have to comply with the following cumulative conditions:

- implement technical and organizational measures, in order to respect the principle of data minimization, but also to enhance data security and appoint a data protection officer,
- determine retention periods depending on the nature of the data and the purpose of the processing,
- periodically train the employees who process the respective data with regard to their obligations.

Nevertheless, this provision does not provide for specific information regarding the measures that need to be implemented in order to mitigate the impact and the correlative risks pertaining to the processing of personal identification numbers. It only refers to generally applicable requirements that would need to be complied with in reference to any kind of processing activity.

Additionally, Law 190/2018 also provides for the conditions that need to be fulfilled when controllers implement video or electronic communication surveillance means for their employees. Similar to the abovementioned issue, except for limiting the retention period for such personal data to 30 days, such conditions represent only a reiteration of the steps that need to be performed when carrying out a legitimate interest assessment, without providing for specific mitigation measures or other restrictions.

Hungary

The comprehensive modification of sectorial legislation was introduced, concerning the amendment of the Hungarian Labor Code, the act on the processing of health related data, modifications concerning security services and activities of private investigators. According to these modifications, electronic surveillance systems may be used exclusively on private areas. The labor code regulated and limited the possibility to ask job applicant for criminal record from job applicants. The employer must be able to justify such request and prepare a necessity and proportionality test. The usage of biometric authorization in a workplace is subject to conditions such as proving that it is necessary to defend life, health of employees, or a substantial protected interest. Proper balancing test shall be pursued in those cases.

Croatia

In accordance with the Croatian GDPR Enforcement Act ("Official Gazette" 42/18; hereinafter: "GDPR Enforcement Act"), specific Croatian provisions are dealing with specific data processing i.e. (i) consent of child in relation to the information society services; (ii) processing of genetic data; (iii) processing of biometric data; (iv) processing of data via video surveillance; (v) data processing for statistical purposes.

In accordance with the GDPR Enforcement Act, it is considered that the processing of data of a child in relation to the information society is lawful in case it is based on the consent of a child aged 16 (or above). Regarding the processing of genetic data, any processing of genetic data in relation to the analysis of possible illness or other medical aspects of data subject in relation to the life insurance agreement are prohibited.

Regarding the processing of biometric data, such processing is strictly limited and such processing (for the private sector purposes) is allowed only: (i) in case such processing is prescribed by law; (ii) is necessary for person or assets protection, for the protection of classified data or trade secrets and only in case that the interest of the data subject do not prevail over such data processing; (iii) for the purpose of work time evidence in case such processing is prescribed by law or in case there is no other alternative for work time evidence and only with the valid consent of the data subject.

In accordance with the GDPR Enforcement Act, data processing via video surveillance is limited for the purpose of person and assets protection and such processing may be conducted only in case that the interest of the data subject do not prevail over such data processing.

Finally, in accordance with the GDPR Enforcement Act, Croatian public authorities and bodies cannot be fined for breach of the GDPR Enforcement Act or GDPR.

Personal data violations reported to Data Protection Authorities

Bulgaria

As per the annual report of the CPDP for 2018, 33 breach notifications were submitted during the year. Such were filed by controllers situated in Bulgaria, as well as in other EU and non-EU countries.

Most of the notified breaches are related to disclosure of personal data to third parties as a result of unintentional technical errors of personnel, or technical problems in information systems used. Other breaches are related to unauthorized access to data, including cyber attacks. The CPDP has also been notified of security breaches related to data on Facebook and Google platforms.

Along with the "human related" types of breach notifications, there has been incidents caused by natural disasters. Most often, physical security incidents are caused by fire in the premises and systems of controllers that destroy files containing personal data.

In 2018, besides the breach notifications filed in Bulgaria, the CPDP cooperated to other supervisory authorities who have requested provision of information, e.g. with respect to notifications submitted to them. Thus, the CPDP has assisted the Hungarian supervisory authority on 5 information requests and the Swiss authority on one.

The Czech Republic

The statistics of the Office for Personal Data Protection show that since the GDPR became effective the number of complaints for the breach of obligations of data controllers and processors filed with it has significantly increased. However, not all of the filings were legitimate.

During the first nine months of the GDPR effectiveness, the office received 3,223 complaints, nevertheless only **626** were eligible for administrative inquiry.

The notifications concerned, for instance, **telemarketing**, **CCTVs**, **bank registers data transfers or obtaining data from the public registers**.

a dramatic change in the structure and the amount of resources allocated to this office.

Slovakia

Currently, this information is not available to the public.

Lithuania

In 2018, the State Data Protection Inspectorate received about 100 data breach notifications (in 2017 – 7, in 2016 – 8), 93 of which were received after 25 May of 2018. Most of the reports were submitted due to the circumstances such as data disclosure (56 cases), data loss (11 cases), data theft (6 cases), data distortion (4 cases), data copying (3 cases) and other reasons (20 cases).

Poland

Approximately 4,000 complaints concerning the violation of the provisions of the GDPR were submitted to the Personal Data Protection Office so far and the number of received data breach notifications is about 2,000.

Data protection violations, which are reported to the Personal Data Protection Office, mostly concern the following situations:

- sending the documentation containing personal data to unauthorized persons (this applies to both e-mail correspondence and paper correspondence);
- loss / theft of electronic media / computers (in many cases it turns out that these devices are not secured or are secured incorrectly);
- improper destruction of documentation by controllers (a frequent phenomenon is a situation when the documentation is not destroyed at the headquarters of the controller or with the participation of a professional company, and is found after some time by third parties in public places or on private premises);
- loss of paper documentation by the controller or his staff;
- hacker attacks resulting in the acquisition and / or encryption of the controller's databases.

Romania

Based on information made public by the Romanian Data Protection Authority during public events, controllers and processors have notified a number of 398 data breaches by way of the standard data breach notification template. The object of such data breaches referred to unauthorized access to personal data, erroneous transmission of invoice related information to other clients and disclosure of patient/client personal data to other individuals.

With respect to the complaints filed, we note that a number of 5260 complaints have been registered with the Romanian Data Protection Authority.

Hungary

No official information is published by the DPA regarding the number of incidents reported and number of complaints filed. Based on non-official information the DPA initiated more than 2.000 investigations so far and 380 incidents were reported.

Croatia

There are no publicly available data (formal or informal) about breach notifications submitted to the **AZOP**.
However, based on the data about breach notifications that were submitted in accordance with the Croatian Data Protection Act i.e. act that was applicable before GDPR entered into force, our assumption is that the most of the breach notifications will concern following sector: online technology and telecoms, education and childcare and media.

Summary

The largest number of complaints concerning the violation of the provisions of the GDPR across Central and Eastern Europe was submitted in Poland. It amounts to approximately 4,000 complaints while the number of received data breach notifications is about 2,000. The Czech Republic sports the second highest score with over 3,000 complaints, of which only 626 were eligible for administrative inquiry. Controllers and processors in Romania have notified a number of almost 400 data breaches, whereas the statistics in Slovenia and Lithuania present a similar level – respectively, there have been 110 and 100 breach notifications. The rest of the examined countries generally have not made available such information. However, the latter's non-official information leads to presume that the Hungarian Data Protection Authority has initiated more than 2,000 investigations and 380 incidents were reported. Reported data protection violations in Central and Eastern Europe concern mostly data loss, theft and unauthorized access to personal data, with particular reference to the media sector.

In Romania, after the authority has initiated over 450 controls, no fines but corrective measures and warnings were imposed. To date, in the Czech Republic 6 fines based on the GDPR are already effective and enforceable. They mainly sanction inappropriate data security and data processing without necessary consent and amount to the sums from approximately EUR 390 to EUR 1,170.

On the other hand, all of the fines imposed in Hungary, regarding approximately 10 cases, range between the amount of EUR 3,000 and EUR 40,000. The case resulting in the maximum amount derived from the failure to report personal data breach and notify the data subjects accordingly – the user data base of a political party containing the names, e-mail addresses and encrypted accounts passwords of the users became accessible via the Internet due to a hacker attack, who made available the information in question on the website.

In Lithuania the Data Protection Authority has recently imposed its first-time fine in the amount of EUR 61,500 on a FinTech company on account of the inappropriate data processing, disclosing of personal data and failing to provide notification on data breach. The company suffered a data breach in July, 2018, when its customers' personal information became available in more than 9,000 screenshots of banking transactions. During the inspection it turned out that only one employee in the company was responsible for security and information management.

Nevertheless, the first ever financial penalty imposed on the basis of the GDPR in Poland (March, 2019) beat the record within Central Europe. The approximate fine of PLN 1,000,000 (EUR 230,000) concerned failure to provide data subjects with information about the processing of their data by the controller. Namely, the company obtained personal data from public sources and processed them for profit.

Accordingly, in all of the countries surveyed within Central and Eastern Europe, with the exception of Slovenia, where drafting local provisions remains in progress, the implementation of the GDPR was introduced in national legal orders, with some particular emphasis on the matters connected with employment relations, surveillance systems and highly regulated sectors.

Contacts

Bulgaria

Miglena Micheva
Managing Associate
Legal
mmicheva@deloittece.com

Czech Republic

Jaroslava Kračúnová
Partner
Legal
jkracunova@deloittece.com

Hungary

Gabor T. Majoros
Managing Associate
Legal
gmajoros@deloittece.com

Lithuania

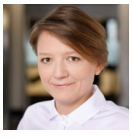
Monika Žlabienė
Managing Associate
Legal
mzlabiene@deloittece.com

Indrė Ambrasūnaite
Associate
Legal
iambrasunaite@deloittece.com

Poland

Zbigniew Korba
Partner
Legal
zkorba@deloittece.com

Agata Jankowska-Galińska
Senior Managing Associate
Legal
ajankowskagalinska@deloittece.com



Ewelina Witek
Senior Managing Associate
Legal
ewitek@deloittece.com

Romania

Georgiana Singurel
Partner
Legal
gsingurel@reff-associates.ro

Silvia Axinescu
Senior Managing Associate
Legal
maxinescu@reff-associates.ro

Slovakia

Dagmar Yoder
Senior Managing Associate
Legal
dyoder@deloittece.com

Croatia

Rado Bekes
Managing Associate
Legal
rbekes@deloittece.com

Jadranka Orešković
Managing Associate
Legal
joreskovic@ovplegal.hr

Katarina Gillich
Managing Associate
Legal
rbekes@deloittece.com

Global, yet grounded

Deloitte Legal Central Europe is

More than
360
legal professionals

operating in
15
countries

collaborating seamlessly

across borders and with other Deloitte business lines

Who we are

As part of the global Deloitte professional services network, Deloitte Legal collaborates with colleagues in an array of globally integrated services to deliver multinational legal solutions that are:

- **Consistent** with your enterprise-wide vision
- **Technology-enabled** for improved collaboration and transparency
- **Tailored** to your business units and geographies
- **Sensitized** to your regulatory requirements

Empowering, collaborative, and pragmatic

Seamless across borders, Deloitte Legal's services are customized to each client's needs. Importantly, we work closely with our clients to plan and deliver our services, enabling them to deliver greater value as an organization.

Corporate and M&A	Commercial Law	Employment Law	Legal Management Consulting
M&A Transactions	Commercial advisory	Compensation & Benefits	Legal Department Strategy & Operations
Integrated Due Diligence	IP for BEPS: Transfer pricing of intangibles	Individual employment law	Legal Technology Consulting
Corporate Law, Corporate Governance	Data protection	International Employment Remodeling	Legal Risk Management
Corporate Reorganizations	Full-Scale Pre-Insolvency Solutions	Human Cloud	Corporate Entity Management
Shareholders Agreement & Joint Ventures	Commercial Contracts	Legal mobility services	Business Integrity
Post-Merger Integration (Legal PMI)	Transfer pricing documentation	Social security	Brexit
Legal & Tax services to startups	Dispute resolution (including tax litigation)		

Regional coordination. A single point of contact

It can be enormously challenging to manage numerous legal services providers around the world and issues can slip into the cracks. As one of the global leaders in legal services, Deloitte Legal works with you to understand your needs and your vision, and to coordinate delivery around the world to help you achieve your business goals.

Regional perspective and local insight

The regulatory environment is only growing more complex. Deloitte Legal Central Europe helps clients advance their enterprise-wide goals with confidence that only comes with the support of an experienced legal advisor with a global span.

We provide meaningful insight and support in jurisdictions around the Central Europe and also bring those together into a strategic perspective that enables and empowers our clients to both meet their local responsibilities and thrive in the global marketplace.

Regional reach, local solutions
Access to the worldwide resources of the Deloitte network combined with in-depth knowledge of local legislation

A sensible, straightforward approach to fees

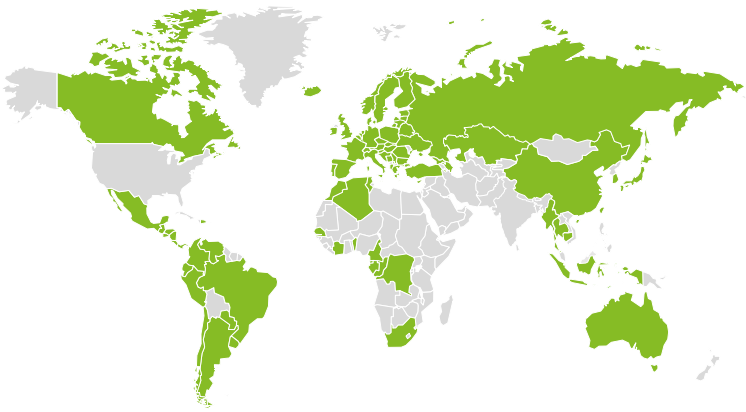
Deloitte Legal Central Europe offers clients numerous fee arrangements tailored for the complexity of the work, such as local or regional preferred rates. This flexibility provides a range of benefits, including:

- improved transparency into your legal services spend
- greater predictability, enabling you to plan for the long run
- intrinsic efficiencies that result from working with a single legal services provider

In addition, our leverage model is distinctive and allows for additional cost efficiencies.

Cross-border coordination and a single point of contact

Deloitte Legal's network of 80+ local practices comprises more than 2,400 legal professionals who collaborate worldwide to cover four major disciplines: Corporate and M&A, Commercial Law, Employment Law, and Legal Management Consulting.



Deloitte Legal practices

1. Albania
2. Algeria
3. Argentina
4. Armenia
5. Australia
6. Austria
7. Azerbaijan
8. Belarus
9. Belgium
10. Benin
11. Bosnia
12. Brazil
13. Bulgaria
14. Cambodia
15. Cameroon
16. Canada
17. Chile
18. China
19. Colombia
20. Congo, Rep. of
21. Costa Rica
22. Croatia
23. Cyprus
24. Czech Rep.
25. Dem Rep of Congo
26. Denmark
27. Dominican Republic
28. Ecuador
29. El Salvador
30. Equatorial Guinea
31. Estonia
32. Finland
33. France
34. Gabon
35. Georgia
36. Germany
37. Greece
38. Guatemala
39. Honduras
40. Hungary
41. Iceland
42. Indonesia
43. Ireland
44. Italy
45. Ivory Coast
46. Japan
47. Kazakhstan
48. Kosovo
49. Latvia
50. Lithuania
51. Luxembourg
52. Malta
53. Mexico
54. Montenegro
55. Morocco
56. Myanmar
57. Netherlands
58. Nicaragua
59. Norway
60. Panama
61. Paraguay
62. Peru
63. Poland
64. Portugal
65. Romania
66. Russia
67. Senegal
68. Serbia
69. Singapore
70. Slovakia
71. Slovenia
72. South Africa
73. South Korea
74. Spain
75. Sweden
76. Switzerland
77. Taiwan
78. Thailand
79. Tunisia
80. Turkey
81. Ukraine
82. United Kingdom
83. Uruguay
84. Venezuela

Deloitte.
Legal