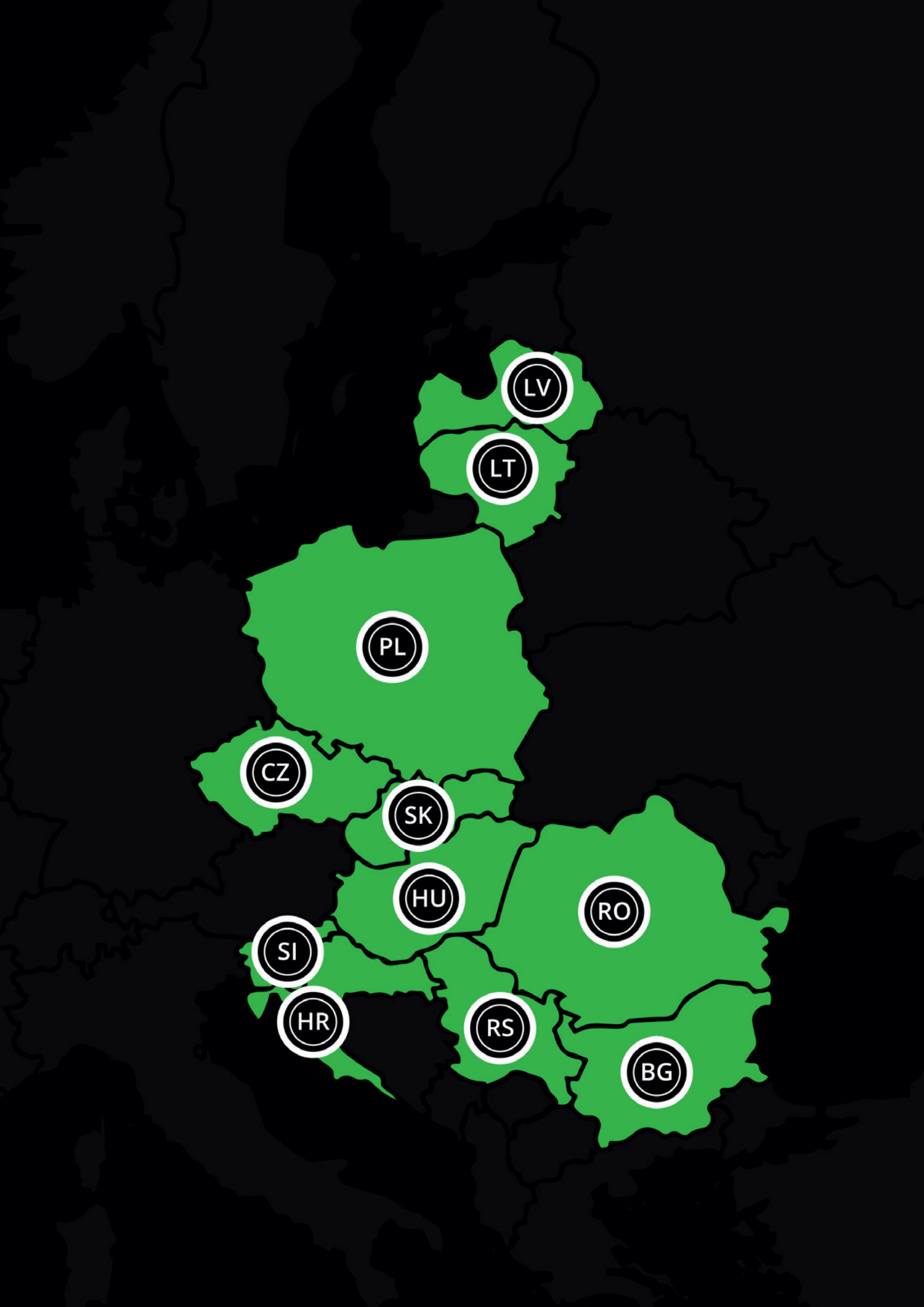
Deloitte.
Legal

The GDPR: Six Months After Implementation

Practitioner Perspectives

Contents


LV
LT
PL
CZ
SK
HU
RO
SI
HR
RS
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. 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 challenges, best practices, sectorial initiatives, regional regulations and the approaches of data protection authorities. The report features a series of insights from Deloitte's experts across Central Europe which are based on their market observations and experiences gained during various projects. We hope you will find this report interesting and useful.

Best regards,

Zbigniew Korba
Partner
Deloitte Legal Central Europe GDPR team

Main challenges observed with regard to application of the GDPR

Bulgaria

The main challenges observed here are:

- The **qualification of a contracting party as a data processor, joint controller or an independent controller** is sometimes challenging and triggers controversy between the parties. We are often contacted by clients who face such difficulties and ask for our advice and assistance during negotiations. These challenges have been addressed by the Bulgarian supervisory authority: the Commission for Personal Data Protection (the "**CPDP**"). In response to several queries the CPDP published opinions regarding the **role of banks, insurers and courier firms**. Their role has been subject to discussions and inconsistent treatment by their contracting parties, i.e. some have treated them as processors and have insisted on signing an agreement under Art. 28 of the GDPR, while others have considered them to be controllers. The opinion of the CPDP is that in most cases such entities should be classified as data controllers, considering that they provide services under strict legal regulations, based on a licence or similar authorisation from the State.

- Determining the legal grounds for personal data processing is also challenging. The CPDP has published **information material on cases in which data controllers should not ask data subjects for their consent** and should use other legal grounds instead. Such examples include: the transfer of personal data from one controller to another as a result of an assignment of receivables; and the processing of personal data in the course of the normal professional activity of banks, insurers, courier firms, doctors, dentists, pharmacists and others.

- Transfer of personal data to a third country is also challenging for data controllers, and we have provided advice to several clients in this respect. The main challenge for controllers is to decide on appropriate grounds for personal data transfer to third countries for which there is no adequacy decision of the European Commission.

The Czech Republic

With regard to the introduction of the GDPR in the Czech market our clients have experienced various challenges in different phases of standard GDPR readiness and implementation projects.

In the initial phase, when it is essential to get to know the details about the processing of personal data within the given client's company, we generally find some entities at times face a **lack of awareness** of basic rules, such as what personal data actually is and what the basic principles of processing are. This is mainly due to historically low enforceability of the local Czech data privacy laws, but we believe that will gradually change due to the GDPR. Therefore we focus our efforts on educating the key people across companies' structures about this particular topic in order to receive complete information needed in order to successfully proceed with the project and to cover all potential risks involved, mainly in the form of risk analysis and gap analysis.

Further within the implementation process itself we experience major challenges in connection with ensuring compliance with the principle of data minimisation, i.e. **data erasure and setting archiving periods** or collection of excessive data without any clear intention of the present use thereof. Introduction of data erasure is particularly difficult in most IT systems used by clients, which were programmed in such a manner that does not allow for data to be erased, or even anonymised. Some of those IT systems may be critical for the given client's business and their modification would require high costs. As for setting retention periods, this task becomes particularly intricate in cases of processing based on the legitimate interest of the controller, where the expiration period derives mainly from business requirements and may vary according to the risk-based approach of the particular company.

Apart from the above, analysis of roles of the different parties with respect to personal data processing, i.e. the controller-to-processor / controller-to-controller / joint controllership relationship, is also challenging in various cases, due to vague legal definitions and lack of case law. The definition of personal data processing **purposes** remains a controversial topic for the same reason, as well as due to the lack of guidance on the part of the supervisory authorities.

As a general observation, there are many misinterpretations of the GDPR taking place in the Czech market, which lead to **excessive usage of consents** for personal data processing in cases where another legal basis is obviously applicable. This has also been noted by the Czech Office for Personal Data Protection, as we explain below in more detail.

As for the main challenge within the post-implementation process, companies continue to struggle with finding the right set-up and resources (both human and financial) for ongoing **consultancy services and internal audits** with respect to data privacy. There is a significant lack of competent staff on the market.

Latvia

- One of the main challenges is the **division of roles between controllers and processors**. Very often service providers do not want to be considered to be processors and want to be designated as separate and independent controllers of personal data, irrespective of their true role. The main reason for this is the complexity of data protection agreements, i.e. the majority of controllers very often impose a huge number of obligations on processors of personal data that are hard to fulfil.

- **If processors refuse to sign data protection agreements**, controllers in Latvia send privacy notices to the respective processors stating the obligations of the processor as 'proof' of meeting of the relevant requirements of the GDPR, i.e. Art. 28(3) thereof.

Slovakia 

The main challenges that have been encountered by the companies in the market here are related to overall personal data governance in the environment of any given company. Such data governance usually includes a Data Privacy Policy at the corporate level incorporated into all of the structures of the company. For companies with more sophisticated organisational structures an **RACI matrix** can be also an essential asset with regard to data governance.

This has been caused partly by the approach taken by most companies, in which they have mostly decided to rely only on the assistance of a legal advisor, which has enabled them to receive basic documentation related to the GDPR (e.g. consents, data processing agreement templates, etc), but a thorough mapping of data flow, a focus on IT aspects of the matter, etc are often lacking.

Lithuania 

In Lithuania there was generally low awareness of the protection of personal data and GDPR requirements, and firms relatively rarely appointed employees responsible for compliance with data protection regulations within their organisations. This represents a challenge for effective governance, as relevant "privacy incidents" might not be identified and relevant policies and procedures might not be used.

Furthermore, the majority of the organisations did not:

- have comprehensive and consistent privacy policies – **different rules on personal data protection and privacy were spread fragmentally in various documents**, which themselves were not sufficient comprehensive;
- ensure sufficient **transparency to disclose all relevant information** about the processing of personal data to data subjects as required under the GDPR – there were issues regarding the scope of information which needs to be provided to data subjects, i.e. many organisations were struggling when looking for a way to provide information in an easily understandable manner, and in clear and plain language, and at the same time ensure that all required elements of information were included in privacy notices;
- have appropriate agreements in place to ensure an adequate protection of personal data (e.g. data processing agreements with data processors and (or) respective agreements with data controllers/suppliers) and did not have a register of data flows, therefore it was challenging to comply with the requirements of the GDPR.

The businesses were also heavily relying on consent as a legal basis for data processing, not being aware that in many cases consent is actually not the proper legal basis for the data processing. We also observed a significant problem with determining the periods of data retention when there are no specific legal provisions of law setting out the exact period.

Poland 

The main challenges observed with regard to the application of the GDPR were the preparation and maintenance of the **records of processing activities**, in particular proper identification of data processing within organisations (data flows, purposes, amounts of data).

Firms have difficulties with interpretation of the GDPR, sometimes resulting in misguided market practices, e.g. **heavy reliance on consents** when such are not an appropriate legal basis for the processing of data. Companies also find the determination of the character of co-operation between two parties of an agreement challenging (i.e. determining whether the co-operation is based on outsourcing of data processing, making the data available by one controller to another controller or joint controllership). New legal obligations, e.g. introducing a **risk-based approach** into the decision-making process and conducting risk analyses, may be sometimes quite challenging.

We also observe a significant problem with determining the **periods of data retention** when there are no specific provisions of law setting out the exact period therefor. Moreover, the matter of back-up management is challenging, particularly setting the **back-up retention** period and defining the legal grounds for processing back-ups after the original data has been deleted.

Moreover, improper GDPR implementation may result in reduced income for companies, e.g. preventing marketing activities. Firms also have difficulties with regard to exercising data subjects' rights when relevant requests are inaccurate.

It is worth emphasising that companies will face many problems with regard to **maintaining continuous compliance with the regulations**. It is necessary to monitor data processing and fulfil obligations imposed by the GDPR, e.g. firms are required to keep up-to-date registers of data processes and ensure that IT systems guarantee adequate data security. Compliance with these obligations involves significant costs for companies. Moreover, in order to monitor data processing, it is necessary to employ appropriate staff, but a lack of adequate human recourses seems to present problems here. Employers sometimes face difficulties with finding qualified employees in the field of data protection, e.g. Data Protection Officers.

Romania 

In terms of GDPR application we have been confronted with the following main types of challenges, which arose both during assessments of the personal data processing activities of our clients and also during the introduction of the necessary compliance documents:

- lack of guidance, recommendations or official positions from the local DPA

in terms of the interpretation of GDPR provisions – most of the time guidelines issued by Art. 29 WP, CNIL, ICO, the Bavarian DPA or international jurisprudence were used as points of reference;

- faulty application of the articles where the GDPR allows the Member States to derogate from its rules, as the relevant Romanian legal acts, in certain cases, fail to reflect the substance of the GDPR;
- drafting **sophisticated and highly-personalised privacy notices, policies or other internal documents** regarding data protection compliance (general data protection policy, procedures for handling requests from data subjects, etc) in lack of any existing templates,
- organisational resistance in terms of the actual introduction of the procedures and compliance measures within companies – understanding the client's business needs and performing tailored trainings related to data privacy for a business's members has been of great use in reducing such resistance;
- balancing and accommodating the business needs of companies and their previous data-privacy-related practices to the requirements of the GDPR without disrupting the business activities – having one-to-one meetings with key business persons (i.e. marketing, HR, customer care, etc) was quintessential in this process.

Hungary

Hungarian data controllers and processors certainly faced several challenges as of 25 May 2018. None of these were major issues endangering business operations but they did cause headaches. Those issues are as follows:

- The failure of the legislator with regard to the timely adoption of the amendment to the local data protection law in order to align it with the GDPR caused a two-month-long "outlaw" period between May 25 and July 25 causing uncertainty among data controllers/processors. In the absence of the appointment of the supervisory body, market players could not decide to what extent should they adhere to the previous regime.
- The Hungarian supervisory body (DPA) has been quite passive with regard to providing assistance to data controllers/processors related to their preparations for the new data protection regime. The DPA issued short resolutions, but those were answers to particular inquiries rather than official guidance to data controllers/processors.
- In our view an issue that should be mentioned is **how previous consent forms may live on after 25 May 2018**. The GDPR's rules are clear in this respect; however, Hungarian consents, in our opinion, oftentimes could not be considered as "consent pursuant to Directive 95/46/EC" as mentioned in recital 171 of the GDPR.
- Data controllers have needed to bear a great burden in order to comply with the GDPR's provisions, e.g. those regarding data processor contracts, joint data controlling contracts, records of processing activities and the introduction of those methodologies and template documents relating to the recordkeeping obligations of data controllers/processors in the event of data breaches and high risk data processing activities. All these – in particular the records of processing activities– are causing significant administrative burdens to the companies involved, requiring great amounts of resources, both human and financial.
- Legal compliance is only one side of the GDPR, and complying with its information security principles oftentimes require serious financial and time investments.

Croatia/Slovenia

- In certain companies, due to the **complexity of major systems** and processes, the process of achieving GDPR compliance takes more time.
- There are also differences in interpretation of the GDPR, which can cause delays in implementation, e.g. in case of determining the **granularity of consents** for personal data processing.
- The local regulator is sometimes stricter than its European counterparts, which increases the requirements on companies here. For example, the local authority has issued opinions that have classified small start-ups that are not incorporated as companes as physical persons instead; therefore the same level of protection for their data (regardless of the fact that they act in a business capacity) needs to be ensured as if they were natural persons.

Best practices observed in the market

Bulgaria

Best practices in the market we have observed so far are:

- Conducting **staff awareness trainings** – we have been engaged to organise such for a large number of clients' employees. Our presentations and the interactive discussions helped employees to become familiar with relevant GDPR requirements and to understand how to apply those in their everyday work. According to information received by other clients, such training sessions have been organised internally too, which shows that businesses are dedicating significant efforts to such practices and consider them useful.
- **Staff involvement in GDPR implementation** – our experience with the GDPR Gap Assessment and Implementation projects shows that clients prefer to engage their employees in the process of bringing their organisation into GDPR compliance. Employees of all levels within these organisations have participated in workshops and other activities we have organised during the projects, which has had many positive effects for both project delivery and enhancing staff awareness.
- **Special system/digital tools for maintaining records of processing activities** – some clients maintain such systems, which are also used for calculation of risk levels regarding all personal data processing activities. Thus not only mandatory assessments are performed, but also a full risk assessment of all activities, which can easily be kept up to date.

The Czech Republic

The majority of companies have understood that the personal data protection regulation is rather not to be underestimated now that the GDPR has come into effect. Such companies view GDPR readiness and implementation projects as a **complex exercise** equal to other compliance projects, accepting even relatively high costs in order to achieve GDPR compliance. Companies invest in systematic mapping of processes that include personal data processing and spreading awareness among their staff, which also serves as a effective preparation for the implementation of the GDPR.

Privacy policies have been amended and the **re-consenting** process has taken place in most companies. Such documents and processes indicate that these companies have gone through a detailed readiness and mapping process, having then systematically identified the purposes of personal data processing inside the respective company and the applicable legal basis therefor.

SMEs, which do not require more than one FTE for an effective execution of the **Data Privacy Officer role**, generally handle awareness very well, dealing with requests from data subjects and change management procedures by setting points of contact, adjusting internal regulations and providing e-learning or regular training courses for key staff. Larger companies, on the other hand, make use of external consultancy support in order to complete the implementation process and cover the consultancy needs prior to establishing sufficient internal human resources.

Template documentation and sophisticated methodologies for compliance with more advanced obligations, such as Data Privacy Impact Assessments or balance tests, are created and followed specifically in companies with innovative means of personal data processing and/or companies whose businesses involve high-risk processing of personal data.

Latvia

- One of the best practices is preparing and **publishing on a company's website forms for requests from data subject** that have to be filled in thereby. This might help companies to deal better with requests from data subjects, because those will be standardised.
- Another of the best practices is a company publishing its r**ecruitment data retention policy online**. The purpose of that is to inform job applicants about the processing of their personal data in the recruiting and hiring process. In this way, pursuant to the GDPR, companies can inform job applicants about the personal data they process, as well as to provide information about data subjects' rights and other necessary information related to the processing of job applicants' personal data.
- Another good example is the preparation of **privacy notices for employees**. The purpose of such notices is to inform employees about the processing of their personal data, including the uses thereof within the framework of employment. In this way, pursuant to the GDPR, companies can inform employees about their rights, personal data processing principles and purposes, and the grounds for personal data processing etc.

Slovakia

From our experience the best practice to dealing with the new regulations and obligations introduced by the GDPR has been to use a **uniform approach of legal, IT and business set-up of internal processes within a company**. Such an approach enables companies to tackle all the necessary aspects of this regulation and connect such within uniform policy/practices regarding data processing and protection, which could help them in the future, e.g. they could achieve a better protection of processed data, co-operation with the regulatory authority could be easier, the responsibilities within the company are more clearly structured, etc.

Lithuania

The most of the businesses have understood that the personal data protection regulation is rather not to be underestimated anymore since the effectiveness of the GDPR. Such businesses took the GDPR readiness and implementation project as a **complex exercise** involving businesses' legal, IT and business capabilities.

Lithuanian Association of DPOs (LDAPA) has been established in Lithuania. It unites and integrates personal data protection and data security experts from the public and private sectors, from businesses and other organisations, whose activities are related to information security and the protection of personal data. The priority of the LDAPA is to create an **innovative, new generation, non-commercial platform to share specialised legal knowledge, good practices**, and practical and creative solutions among personal data protection specialists. The LDAPA is the first association in the field of personal data protection in Lithuania.

We believe that another of the best practices observed in the market here relates to transparency requirements introduced by data controllers. Due to the GDPR transparency requirements many data controllers have started using layered privacy statements/ notices in an online context, as those enable data subjects to navigate to the particular section of the privacy statement/ notice which they want to immediately access rather than having to scroll through large amounts of text when searching for particular issues. Thus information on personal data processing is provided in a concise and transparent manner, as required by the GDPR.

Poland

We find it that satisfying that firms have introuced comprehensive internal regulations concerning data protection, including policies, procedures and registers. Moreover, consents have been renewed to comply with the GDPR and companies have prepared and delivered the informational obligation under Art. 13 and 14 of the GDPR. In our survey in the banking sector, most of the surveyed banks have fulfilled their obligations before first contact with a given client.

Data subjects tend to exercise their rights more often. It has been noted that the right to be forgotten is even excessively used. In general, controllers respect the exercising of data subjects' rights.

The introduction of **security measures that go beyond the required minimum standards** (for example the encryption of all the documents attached to e-mail) is also considered to be a good practice. Moreover, GDPR implementation often entails the development of **new technological solutions** enabling appropriate data protection and has had a significant impact on the increasing awareness of data protection.

Romania

In terms of best practices available at the level of the Romanian market we note that we have not identified such practices locally.

Generally the Romanian market is influenced in its data privacy related to compliance by the best practices mentioned by other DPAs, Art. 29 WP and jurisprudence of the ECHR or CJUE, which are promoted by the privacy consultants or lawyers handling the respective issues.

Hungary

It is a general truth that during the course of processing personal data business entities have to comply with regulatory requirements, but it is also strongly recommended to adhere to market best practices. Moreover, oftentimes best practices are established by supervisory authorities, including WP29 and the DPAs of Member States.

We are not aware of any followed best practices originating from the private sector, thus we can say that business here **follows the known practices issued by WP29 and/or National DPAs.**

Croatia/Slovenia

- Good practice in **evaluation of processors and processor audits**, easy to use excel tool for establishing controller-processor relationship and assessing the risk for specific processor.
- Good practice in granulating consents and establishing consent management system.
- Good practice (confirmed with regulators) on **split between direct marketing and segmented and targeted marketing**.

Actions taken by supervisory authorities

Bulgaria

The CPDP has organised several **public events**, e.g. awareness events and training sessions, as well as the 40th International Conference of Data Protection and Privacy Commissioners. It has also published information materials and opinions on several queries made by private entities and public authorities. In addition to the opinions mentioned above regarding the role of banks, courier firms and other controllers, the CPDP has provided an opinion to a bank with respect to its intention to introduce **voice recognition** in its call centre in order to address requests from clients that require customer authentication.

The Czech Republic

To date no fines have been imposed due to breach of GDPR regulations by the local supervisory authority, i.e. the Office for Personal Data Protection.

Inspections are being conducted in a relatively limited scope and include the public and private sectors. The representatives of the Office for Personal Data Protection say that the primary focus of the office is currently on **consultancy and support to the market, rather than inspections and imposing penalties**. Its personnel regularly appear at educational public events.

The chairwoman of the Office for Personal Data Protection recently issued an official statement regarding the excessive usage of consents for personal data processing, which is clearly a malpractice noted by the office and will be combated by the office.

A previous statement from the chairwoman also emphasised the importance of improving the data privacy culture and **accountability** within companies, stating that future inspections may focus on that rather than on shortcomings of particular processing scenarios.

It is also important to stress that the Czech Office for Personal Data Protection suffers from a significant capacity shortage, which has already the situation for some time. This should change with the adopting of the local adapting law, which promises a dramatic change in the structure and the amount of resources allocated to this office.

Latvia

- There is no publicly available information about fines and decisions taken.
- The Latvian Data State Inspectorate has prepared a notification form (an excel file) for **notification of personal data breaches** (available only in Latvian). Use of this form is not mandatory.

Slovakia

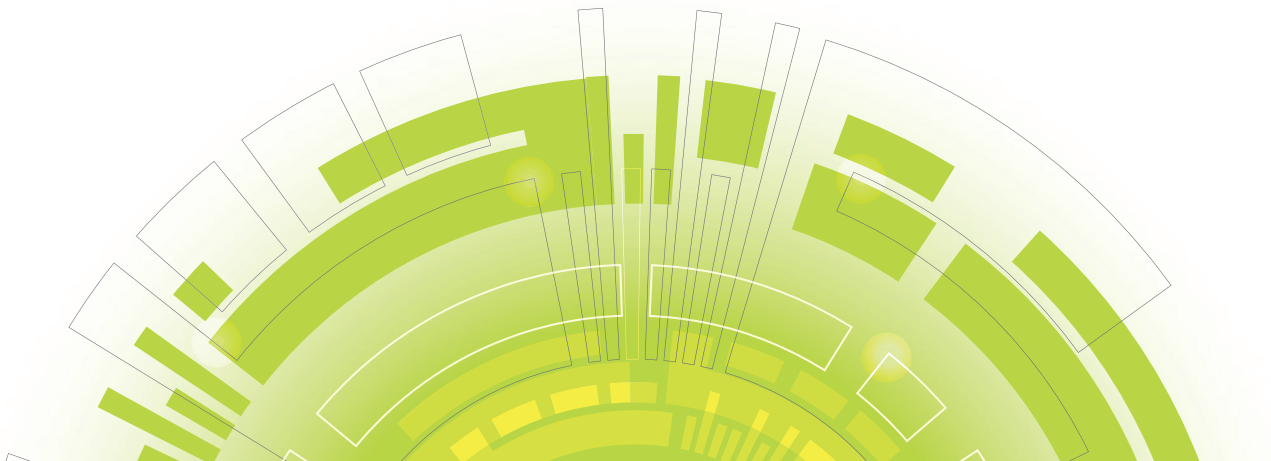
We have no knowledge of any inspections carried out or fines imposed by our supervisory authority. This is partly caused by the fact that there have been mixed opinions regarding the approach to be taken in relation to inspections and fines after the GDPR became applicable.

The supervisory authority seems to be taking a somewhat static approach and is **expected to start the inspections from 2019**, so as to give companies time to take necessary measures in order to be compliant with the new legislation. However, this approach has not been officially communicated by the supervisory authority, it is just an observation of the situation on the market.

Lithuania

During 2018 the Lithuanian supervisory authority, i.e. the State Data Protection Inspectorate (the "SDPI"), received 644 complaints regarding data processing activities, mostly related to direct marketing, surveillance data and data processing activities in the Internet. As a result thereof the SDPI performed 139 inspections on data controllers.

The SDPI has released a summary of the results of one inspection. That inspection was carried out with regard to marketing activities of major companies



operating in the food, household products stores and pharmaceuticals sectors. The SDPI identified violations regarding data processing activities performed in all of the inspected companies. The SDPI provided instructions to the inspected companies on how to eliminate the identified violations and no fines have been imposed to date.

Furthermore, the SDPI, contributing to the process of personal data protection reform in Lithuania, has prepared 15 legal acts and harmonised 395 legal acts and documents of data controllers. The SDPI has also prepared and published several different guidelines and opinions covering different topics related to privacy:

- **guidelines for small and medium-sized businesses** which are aimed at helping them to apply new legal regulation on personal data protection in practice;
- an opinion on the application of the GDPR to the processing of **personal data of members of management bodies** of legal persons;
- an opinion on the obligation to appoint a Data Protection Officer (DPO);
- an opinion on identifying, investigating, reporting and documenting personal **data security breaches**;
- an opinion on records of data processing activities;
- an opinion on requirements for a draft law which will regulate the processing of personal data.
- The SDPI has also provided **sample document templates** for several issues related to the GDPR, i. e.:
- a template for a request for permission to transfer personal data to third countries or international organisations;
- a template for a report on a security breach involving personal data;
- a template for the procedure for the implementation of data subjects' rights.

Use of the above-mentioned templates is not obligatory. However, they are highly recommended by the SDPI.

Finally, the SDPI and Mykolas Romeris University have started a project for the promotion of high standards of personal data protection in Lithuania. The project is called "Solving Privacy Paradox: promotion of high standards of personal data protection as a fundamental right and one of the key factors for consumer confidence in the digital economy (SolPriPa)".

Poland

The Polish supervisory authority has launched many initiatives to support the implementation of the GDPR by companies here. First of all, the President of the Data Protection Office has issued a **number of guides**, e.g. a guide on data protection in **schools**, a guide on data protection during **election campaigns**, a guide to data protection in the **workplace**, a GDPR guide for the public health service and a guide on conducting **risk analysis**.

The authority has also organised training sessions, e.g. for Data Protection Officers, judges, public officers and NGOs. The supervisory authority was also the organiser or a co-organiser of numerous conferences regarding data protection. There are also initiatives targeted at schools, e.g. competitions and training materials.

The President of the Data Protection Office has carried out inspections regarding GDPR implementation, starting with public registers, followed by the medical and education sector, as well as controllers

Romania

The Romanian supervisory authority has historically been much less active than most of the other European supervisory authorities. As such, in the last few months the supervisory authority has not issued any publicly available information about any fines imposed for any non-compliance arising out of or in relation to the provisions of the GDPR. However, we note that the Romanian supervisory authority has doubled its budget from last year and is looking to double the number of its employees, thus becoming more efficient in its tasks.

In terms of initiatives, the Romanian DPA has only issued the following:

- **a guide on the position of DPO** (the guide reflects the provisions of the GDPR and the guidelines of Article 29 Working Party, without issuing any supplementary clarifications; moreover, such guide is of a nature that creates confusion, in the sense that it recommends that all companies, regardless of whether they satisfy the relevant conditions provided by the GDPR, appoint a DPO);
- **a complaint-filing procedure**, along with a complaint template which must be used when submitting an electronic complaint;
- **a breach notification form** (which can be submitted only online, and signed only via an electronic signature) which must be used for compliance with GDPR-related duties;
- an investigation procedure to be used by the Romanian DPA when carrying out investigations; and
- a list regarding the processing activities for which a DPIA must be performed.

Moreover, the Romanian DPA has withdrawn all of its previous decisions related to national restrictions regarding the processing of personal data regarding personal identification numbers, CCTV, etc.

On 11 September 2018 the DPA published its report on the activity it carried on in 2017 (based on the previous data protection framework). The number of complaints registered with the DPA, and the investigations initiated by the DPA pursuant to such complaints or ex officio, had gone up significantly as compared with previous years. With respect to complaints or investigations followed after the entering into force of the GDPR, the DPA has already made publicly available information that during the four months after 25 May 2018 1,643 complaints had been registered and there are numerous pending investigations.

Hungary

The Hungarian DPA has not been too active since 25 May 2018. For the first two months, in the absence of its official appointment as the local supervisory authority, the DPA simply did not have the regulatory authorisation to proceed in any cases concerning GDPR provisions.

According to prominent DPA officials the DPA is well aware of its insufficient assistance provided to data controllers/processors, thus the authority does not plan to launch sizeable campaigns of administrative proceedings/inspections. This somewhat contradicts recent news reports, according to which the DPA has initiated proceedings against two major players in the FSI sector.

What the local DPA had been doing was issuing sets of short resolutions in which the **DPA answered particular inquiries**. These resolutions reflected practical questions, including, but not limited to, the following:

- a **DPO's required professional skills** and his/her recommended position within an organisation;
- data processing activities of municipalities;
- the applicability of the GDPR in the legal profession; data-protection-related tasks (records of processing activities, impact assessments) for private business entities;
- actions for family doctors to take;
- the **applicability of the GDPR in the SME sector**;
- language of notifications to be provided for employees;
- language of notifications on data protection incident to be submitted to the Hungarian DPA, etc.

The Hungarian DPA recently stated that only the European Data Protection Board is entitled to interpret the GDPR, therefore it will cease its related activity.

Croatia/Slovenia

- Regulators were primarily focused on education and establishing the system of GDPR implementation (opinions, frameworks, templates, etc.)
- Information from the market (communication with the regulators) is that the controls of the implementation are starting soon – presumably not in this year.

Sectorial initiatives taken

Bulgaria

The **Bulgarian Supreme Bar Council** has published various materials to help lawyers (generally being controllers) in the process of GDPR implementation, among which are templates for internal data protection rules, statements granting consent, data protection agreements with data processors, etc.

The Czech Republic

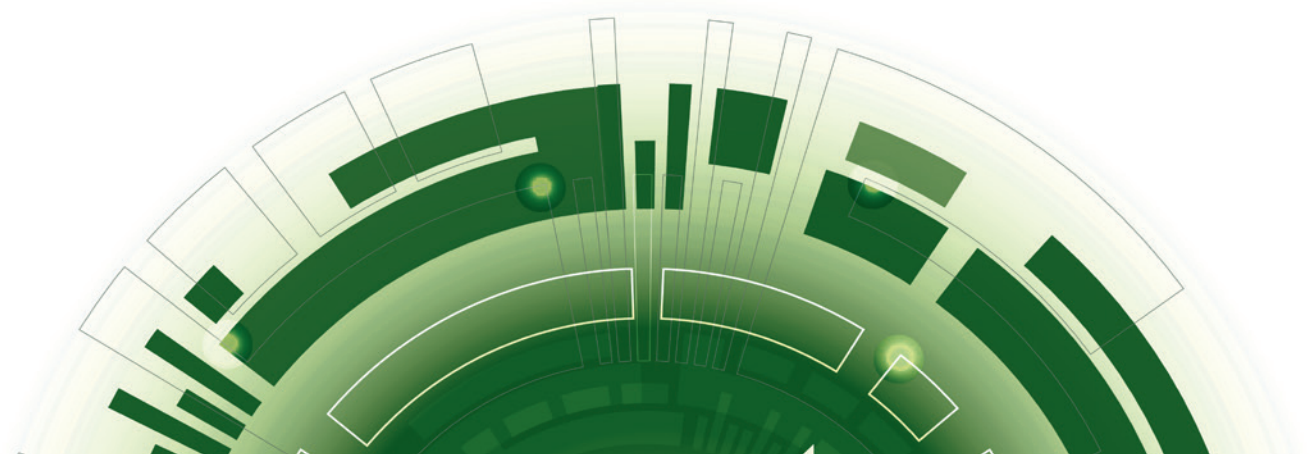
We have noted several sectorial initiatives in the field of the GDPR in the Czech Republic, mostly covering the preparation of codes of conduct under Art. 40 of the GDPR and guidelines for the sectors involved. Among these initiatives are the following:

- APEK (the **Association for E-Commerce**) is preparing a GDPR code of conduct for online shops;
- the **Association of Small and Medium-Sized Enterprises and Crafts** is preparing various GDPR tools, e.g. GDPR guidelines for small and medium enterprises together with the Ministry of Industry and Trade;
- the Czech **Traditional Retail Association** is preparing a code for personal data protection;
- the **Association of Personal Services Suppliers** is preparing a code for the personal data protection; and
- various professional associations have reacted to the GDPR by providing their members with at least general guides on how to approach the GDPR, including the Chamber of Auditors of the Czech Republic (articles and FAQs), the **Czech Bar Association** (a guide, FAQs and sample documents for attorneys), the Czech Chamber of Commerce (a guidebook and lectures) and the Czech **Medical Chamber** (sample documents and a guide).

The Czech Office for Personal Data Protection has published various materials, such as statements, FAQs and guidelines, which are, however, mostly cross-sectorial.

Latvia

- The Finance Latvia Association has prepared comprehensive **guidelines for personal data processing by banks**. Particular attention is paid to the main aspects of banks co-operation with clients:
  - the specific types and amounts of customer data – the guidelines specifically highlight the processing of the certain personal data (health data, information on membership of trade unions, data of politically significant persons, biometric data, passport copies, children's personal data, and personal data on convictions) and set out when this information could be requested by the data subject;
  - a wide range of services offered – the guidelines highlight that a wide range of services are offered, for example human resource management, provision of credit institution services to customers, marketing, risk assessment, economic and administrative services, etc.;
  - the **bank-customer-specific relationship** – the guidelines focus on the purpose and extent of personal data processed by banks, and the guidelines stipulate that the minimum possible amount of personal data should be requested and also determine the rights of the data subject;
  - **IT systems involved in banking** – the guidelines set out the requirements that banks need to satisfy in the field of IT, for example in order to ensure the protection of personal data it must be protected by firewalls and anti-virus software must also be installed. The guidelines also set out that when information containing personal data is being transferred, the data must be encrypted. The guidelines suggest that there should be a mechanism for the deletion of person data from portable devices if such are lost or stolen. The guidelines also set out that data must be duplicated using back-up solutions (so as to ensure that the data does not disappear), personal data must have physical



protection (protection in the event of a flood or fire, physical protection of the server premises against unauthorised access thereto, the protection of portable media, such as USB drives and CDs, must be ensured).

- The Latvian Personnel Management Association has also developed **guidelines addressing issues involving human resource management**. These guidelines focus on the following topics:
  - the legitimate interests for processing of personal data of employees – the guidelines suggest a few possible legitimate interests for the processing of personal data, for instance human resource management, to ensure efficiency, to ensure the safety of individuals, to take administrative action, to provide services/products and information system operations, to ensure communications and marketing, to conduct audits, and to ensure verification of facts/situations;
  - transfers of personal data – the guidelines set out how and what kinds of information can be transferred to third parties (other controllers) or processors;
  - requirements for IT systems – the guidelines set out the requirements that should apply to the processing of personal data of employees (for example the access system must be set up so that the amount of access can be determined and does not exceed the required amount, each employee must have his/her own access (username and password), data must be duplicated using back-up solutions, while transferring information containing personal data such data must be encrypted, etc);
  - activities in specific situations – the guidelines specifically set out how employee data processing should be performed with regard to specific HR matters (for instance calculating and paying salary, personnel development issues, cases of disciplinary action, communication matters, issues of corporate culture and processing personal data in co-operation with trade unions). The guidelines set out procedures for the storage of personal data, cover who can process personal data of employees, etc.
- The Certified Data Protection Specialists Association of Latvia, which includes DPOs from Deloitte Legal Latvia, is currently working on **guidelines for educational institutions** related to the processing of personal data (pro bono).

Slovakia

We have no knowledge of any sectorial initiatives to date. We understand that there has been some activity in the **banking sector, mainly in relation to DPIAs**, but apart from that we have not come across any significant activity (e.g. codes of conduct or suchlike).

Lithuania

Some associations are thinking about preparing GDPR-compliant code of conducts. However, there are no approved and publicly announced codes of conduct yet. The Lithuanian Bar Association has published guidelines to help attorneys at law (generally being controllers) in the process of the GDPR implementation.

Poland

There are sectorial initiatives in the field of the GDPR. The President of the Data Protection Office has concluded co-operation agreements with organisations representing sectorial interests. For instance an agreement between the authority and the Internet Sector Employers Association has been concluded. The aim of that co-operation is to develop a code of conduct on the processing of personal data in the Internet marketing sector. Such draft is subject to public consultation. Another initiative has been started by the Polish Bank Association, which has been working on a **code of conduct with regard to data processing by banks and in credit registers**.

The **medical sector** has been working intensively on a code of conduct on data processing by small healthcare facilities. And a draft of a code of conduct on processing of personal data for the purposes of scientific research by biobanks in Poland is subject to public consultation.

Romania

We have not identified any sectorial initiatives in the field of the GDPR. However, most probably such initiatives should arise in relation to the medical, financial (i.e. banking and insurance), pharmaceutical and educational sectors.

Hungary

We are not aware of any sectorial initiatives originating from the private sector; most probably the reason for the lack thereof is the absence of a sufficiently detailed regulatory environment. However, draft legislation has been recently prepared to align and harmonise certain laws with the rules of the GPDR, but this proposed act is not considered complete and leaves many crucial data protection issues open, e.g. it does not align the rules of unsolicited marketing communication to the new data protection regime.

Local regulations complementing GDPR

Bulgaria

Amendments to the Personal Data Protection Act have been proposed and recently passed their first hearing at the Bulgarian Parliament. The main area addressed therein is the **processing of personal data of employees** – for example employers are forbidden to copy employees' ID cards and driving licences, unless applicable law provides therefor. In addition, according to information announced by the CPDP it is going to prepare methodological instructions regarding technical and organisational measures for personal data protection.

The Czech Republic

Until now Act No. 101/2000 Coll., on the protection of personal data, as amended, has been regulating the field of personal data protection in the Czech Republic. As of the date of the preparation of this report the above-mentioned act formally still remains in force.

The local law which will replace Act No. 101/2000 Coll. and adapt the Czech legal environment to the GDPR is currently undergoing the legislative process and is in the comments procedure before the Chamber of Deputies of the Parliament of the Czech Republic. The expected timeframe for the effectiveness of the adapting law is Q2/19. The current content of the proposed adapting law focuses rather on the clarification of **personal data processing rules in the public sector**, and it will have no major impact on the private sector.

Latvia

- The law on personal data processing has entered into force; however, it mainly supplements the GDPR. The new law mainly addresses the competence, structure and functions of Latvian Data State Inspectorate.
- In addition, the new law lays down the exemptions and derogations necessary for the purpose of **journalistic, academic, artistic and literary expression**; however, the provisions there are unclear and vague. For instance, even in these cases, there are no derogations from Art. 5 of the GDPR, which covers principles of data processing. According to the principle of lawfulness, fairness and transparency, personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject. According to Art. 6 of the GDPR processing is lawful only if there is an appropriate legal basis therefor. Thus, prima facie, it seems that journalists still might need a legal basis for processing personal data. Moreover, a list of cumulative conditions has to be met in order to apply derogations necessary for the purpose of journalistic expression. One of these conditions states that this derogation will be applicable only if compliance with the provisions of the GDPR is not compatible with or prevents the exercise of the right to freedom of expression and information.
- The new law also states **limitation period for civil law claims related to the wrongful processing of personal data**: five years from occurrence of the infringement. If an infringement is continued: 5 years from the date the infringement ceases to exist.

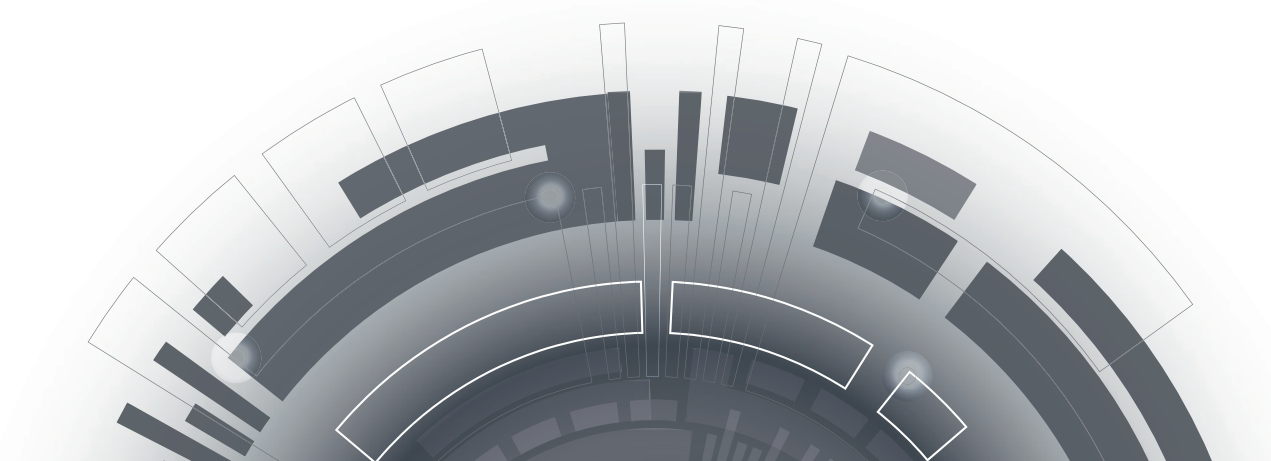
Slovakia

A new act on personal data protection (i.e. Act No. 18/2018 Coll. on Personal Data Protection) has been adopted in our jurisdiction. This new act on personal data protection follows the structure of the GDPR and introduces only minor changes in the fields where GDPR permits such diversion. The changes mainly concern the processing of the **individual personal numbers** of natural persons, which is generally forbidden and the processing of personal data by governmental organisations, and provides further definitions of specifics for the Slovak market.

Lithuania

Before 25 May 2018, when the GDPR came into force, the protection of personal data in Lithuania was mostly governed by the Law on Legal Protection of Personal Data (the "LPPD Law"). After GDPR's entry into force, the LPPD Law was drastically amended and the new wording of the LPPD Law came into force on July 16.

The majority of questions related to legal protection of personal data are directly governed by the GDPR. However, the LPPD Law establishes some peculiarities for data processing, specifically related to the processing of **personal identification numbers and processing of personal data for the purpose of freedom of expression and information**. The LPPD Law also sets specific requirements applicable to personal data processing in the context of **employment relations** and establishes the age limit



for children to whom information society services can be offered.
Below is more detailed information on the provisions of the LPPD Law:

- **Processing of personal numbers**
  The LPPD Law prohibits the processing of national identification number for direct marketing purposes and making ID numbers public. Personal identification number smay be processed only if there is a legal basis for processing as set forth in the GDPR.
- **Processing of employees' personal data**
  The LPPD Law forbids the processing of a candidate's data on convictions and offenses unless it is necessary to verify that the candidate meets certain requirements for employment or duties required by applicable law. Additionally, potential employers may collect information on a candidate's qualifications, professional skills and business characteristics from former employer(s) only if the candidate is informed thereof and from the current employer(s) only with the candidate's consent therefor. Furthermore, in case of video and/or audio data processing in the workplace and on the premises or in the territory where employees work, as well as in the case when employer is monitoring employees' behaviour, location or movement, employees must be informed of such processing and their signature confirming such must be obtained.
- The LPPD Law also states that when personal data is processed for journalistic purposes or the purposes of academic, artistic or literary expression, most of the GDPR's requirements do not apply to such processing. Furthermore, the LPPD Law indicates that information society services can be offered to children only if they are no younger than 14 years of age.

Poland

The Polish government has adopted the Data Protection Act dated 10 May 2018 (hereinafter referred to as the "DP Act"). The DP Act sets forth, inter alia, the obligation to designate a data protection officer and the procedure for notification of his/her designation. Under the DP Act **public sector entities**, research institutes are required to appoint a data protection officer. The DP Act sets a 14-day period after DPO designation in which to notify the Chairman of Data Protection Office thereof. If he/she is replaced or dismissed, the Chairman of Data Protection Office must be notified thereof within the same period.

The DP Act sets criteria and requirements for **certification mechanisms and procedure for the accreditation of a body authorised to issue certifications** in the field of personal data protection, accredited by the Polish Centre for Accreditation. The information to be included in an application for certification and the procedure for verification of an application are also specified in the DP Act.

The GDPR delegates to the Member States the power to set the procedure for the approval of the **codes of conduct** regarding certain aspects of personal data protection. Under the provisions of the DP Act the President of the Data Protection Office approves such codes of conduct.

The Polish government has decided to change the office of the authority responsible for data protection. According to the Act the President of the Data Protection Office is the competent authority. The President of the Data Protection Office is assisted in the performing of his/her duties by the Personal Data Protection Office. Furthermore, the DP Act sets forth the structure of such office. Where that is justified by the nature and number of cases relating to personal data protection in a given area, the President of the Personal Data Protection Office may establish local bureaus of the office.

The **Personal Data Protection Board**, which is an advisory and opinion-giving body of the President of the Office, has also been established in Poland.
The act on the implementation of the GDPR amends more than 160 existing legal acts governing multiple sectors.

Romania

Law No. 190/2018 in respect to the application of GDRP was adopted on 17 June 2018. The law includes, inter alia, provisions regarding the processing of **personal identification numbers based on legitimate interest**. In such case the controller will have to comply with the following cumulative conditions:

- introducing technical and organisational measures in order to respect the principle of data minimisation, as well as enhancing data security and appointing a Data Protection Officer;
- determining storage periods depending on the nature of the data and the purpose of the processing, as well as the time limits after which the personal data must be erased or reviewed for erasure;
- periodically train the employees who process the respective data regarding their obligations.

Law 190/2018 also restricts the processing of data through **audio/video surveillance of employees** by limiting the storage period for a maximum of 30 days, with the exception of specifically regulated cases. Additionally, this law mentions that the certifying bodies for codes of conduct and other certification mechanisms in accordance with the GDPR must be accredited by RENAR (a Romanian accrediting association).

Furthermore, Law No. 129/2018, regulating the aspects regarding the **organisation of the Romanian supervisory authority** (e.g. the responsibilities of the president of ANSPDCP), was adopted on 15 June 2018. That law also details the procedures that will be followed by the Romanian DPA throughout its activities (e.g. the procedures to be followed in case of inspections being carried out or if a data subject brings a claim against a controller or an operator).

Hungary

The GDPR is a source of law containing "general" rules. Naturally, specific areas require such specific rules that complement the general rules of the GDPR.

The Hungarian legislator has recently released a proposal to amend those laws affected by the GDPR. Although the proposal has not been passed yet, it **will affect important sectorial laws**, e.g. the Labour Code, the Credit Institutions Act, the Act on the Processing of Health Data, the Copyright Law, the Act on Electronic Communications, the Act on Security Services and the Activities of Private Investigators (regulating the operation of CCTV and electronic access control systems), the Act on the National Tax and Customs Administration, the Act on Complaints and Notifications of Public Interests (Whistleblowing Act), the Insurance Act, the AML Act, etc.

Certain important sectorial laws, however, remain untouched by the proposal, meaning that we are still awaiting the amendment of, for example, the Act on Commercial Advertising Activities (containing provisions concerning eDM and DM activities) and the Act on Electronic Commerce and on Information Society Services.

The Hungarian legislator has already adopted an amendment of the Act on the Right of Informational Self-Determination and on Freedom of Information (the Info Act, the local data protection law). This amendment significantly modified the earlier wording of this law and extended the scope of the regulation to paper-based data processing activities and to those not falling under the scope of the GDPR.

Croatia/Slovenia

The drafts of data protection laws generally state that GDPR provisions apply and no additional provisions of relevance have been added, except for certain details with regard to video surveillance and maximum periods of data retention.

Activities subject to DPIA

Bulgaria

The CPDP has not published such lists so far. However, regarding the list of activities that are subject to obligatory DPIAs, information available on the official website of the European Data Protection Board (the "**EDPB**") states that such a list for Bulgaria has been prepared. The EDPB has reviewed it and has given an opinion on several activities included therein. For example, the draft list submitted by the Bulgarian CPDP for the opinion of the EDPB envisages that the processing of **biometric data for the purpose of uniquely identifying a natural person, in conjunction with at least one other criterion, requires a DPIA**, and on this point the EDPB acknowledged that the list aligns with the aim of consistency. After considering the opinion of the EDPB and finalising the list, the CPDP should announce it.

The Czech Republic

The Czech Office for Personal Data Protection has decided not to publish an exhaustive list of activities that are subject to DPIAs or exempted from DPIAs. However, in Q1 2018 the office published a draft methodology providing a thoughtful procedure (test) regarding how to assess whether a process is or is not subject to an obligatory DPIA. The test is based on a list of criteria related to the processing of personal data involved, whereby each possible response is assigned a value and the result of the test is then a calculation of the values obtained. The above-mentioned criteria include: the **character and vulnerability rate of the concerned data subjects; the nature, sensitivity rate, scope and quantity of the processed personal data**; and other factors.

At the time of the preparation of this report we are expecting a revised version to be published by the Office for Personal Data Protection following the communication procedure of the European Data Protection Board, as presumed by the GDPR.

Latvia

The Latvian Data State Inspectorate has not published such a list. Nevertheless, this list should be published relatively soon, since Opinion 14/2018 on the draft list of the competent supervisory authority of Latvia regarding the processing operations which are subject to the requirement for a DIPA prepared by the European Data Protection Board is already available.

Slovakia

The Slovak supervisory authority has not to date published such a list. However, there has been unofficial information that such a list might be published by the end of 2018. In this respect the Slovak supervisory authority has managed to publish an ordinance on DPIAs, as a very basic support document to help conduct such assessments. In general, the **ordinance on DPIAs specifies the content of documentation concerning DPIAs**, which should include:

- a description of processing;
- an assessment of necessity and proportionality in connection with the measures to demonstrate compliance with applicable law;
- risk assessment regarding the rights of a natural person in connection to the risk mitigation measures;
- monitoring and revision.

Lithuania

The draft of such a list has been published and presented to the public, stakeholders and data controllers for public consultations. Based on the draft list, **recording of telephone conversations, processing of biometric and/or genetic data, processing of personal video and/or audio data in the workplace**, on the controller's premises or in areas where employees work, processing of personal data related to monitoring of employees, their communication, behaviour and/or movement and similar activities would be subject to obligatory DPIAs. The list is expected to be approved by the Director of State Data Protection Inspectorate and to come into force by the end of 2018.

Poland

In August 2018 the President of the Data Protection Office issued a communication indicating the areas of data processing operations that require data protection assessments.

The list includes nine categories of processing operations which are subject to the requirement for data protection impact assessments, with examples of data processing operations where a high risk of infringement may occur and examples of areas involving such operations. The main areas subject to mandatory DPIA include, inter alia, **profiling and prediction of behaviours that may affect rights and obligations of data subjects, automated decision-making that has a legal, financial or other important impact on data subjects, systematic surveillance on a large scale, processing of sensitive personaldata and information on convictions**, processing on a large scale (taking into account the number

of data subjects, the scope of processing, the retention period and the geographical scale), **profiling and assessment of personal qualities based on data from different sources, whistleblowing systems, systems used for presenting offers based on personal qualities, and innovative use** of technological or organisational solutions.

Romania

The Romanian DPIA has recently published the list of processing activities for which the prior performance a DPIA is considered to be necessary. Generally, the processing activities for which an impact assessment is required refer to systematic and extensive monitoring, or **monitoring of large-scale sensitive data, processing on a large scale personal data through new applications/IoT for the assessment of the financial/ health/etc status of an individual, or processing large-scale/systematic telephony data, internet, metadata or location**.

The Romanian DPIA has not published a list of processing activities for which the prior performance of a DPIA is not considered to be necessary.

Hungary

No. However, the DPA has already submitted to the European Data Protection Board a draft list of those high risk data processing activities subject to obligatory DPIAs. Although the list has not yet been published locally, seemingly the local DPA considers the following processing activities to be high risk:

- processing of **biometric data**;
- processing of **genetic data**;
- processing of biometric "and" genetic data;
- processing of **location data**;
- processing of **data collected via third parties** (Art. 19 of the GDPR);
- employee monitoring;
- processing using new/innovative technology.

In the opinion of the EDPB the draft list of the Hungarian DPA may lead to inconsistent application of the requirement for a DPIA and it recommended particular changes to the draft list.

Croatia/Slovenia

The list is comprehensive and includes, in particular:

- processing of personal data for systematic and **extensive profiling or automated decision making**;
- processing of special categories of personal data for profiling or automated decision making;
- processing of personal data of children for profiling or automated decision making or for marketing purposes;
- processing of personal data by using systematic monitoring of publicly available places on ain large scale;
- **use of new technologies** or technological solutions for personal data processing;
- processing of **personal data generated by sensor devices transmitting data over the Internet** or other information transfer technologies;
- processing of **biometric and/or genetic data**;
- processing of personal data in a manner that involves monitoring the location or behaviour of an individual.

How are data controllers dealing with regulations regarding profiling?

Bulgaria

Regulations regarding profiling are widely noted in heavily regulated sectors, such as the financial services sector.
For example, controllers from this sector are facing challenges when **deciding on the appropriate legal grounds** for personal data processing in cases of profiling for analytical or statistical purposes, as well as for segmentation of clients (e.g. VIP clients).

The Czech Republic

To our knowledge, qualified profiling requiring consent to be obtained has not caused major issues in the market, due mainly to two reasons.

Firstly, the above-mentioned rule is applicable solely to a very narrow scope of real situations, as **most of the profiling that takes place in the market does not meet both of the relevant criteria set forth in Art. 22 of the GDPR**. Such profiling either involves human intervention or does not produce legal effects concerning the data subjects or similarly significantly affect them.

Secondly, those situations of qualified profiling which actually fall into the scope of Art. 22 of the GDPR had, to our knowledge, mostly already been covered by data processing consents prior to the GDPR coming into effect.

Slovakia

Profiling is commonly used in, for example, the banking and insurance sector, and companies from these regulated sectors have also widely used profiling in the past. The obtaining of consent for the conducting of profiling would again depend on the type of a given processing operation, and, to our knowledge, consent for profiling is not always obtained by the companies involved, since it might constitute quite an administrative burden and increase the costs of such operations. Therefore a practice has been identified in which companies look for another legal basis to conduct profiling, e.g. legitimate interest.

There are also other sectors in which profiling is used, e.g. sale of products, etc.

Lithuania

Data controllers, such as banks, insurance companies and others, **usually perform data profiling activities based on the data controller's legitimate interest, compliance with a legal obligation, performance of an agreement or consent from the client**. Profiling activities are commonly described in a given organisation' privacy policies and data subjects are provided with necessary information on profiling activities as required by the GDPR. Analysis for client advice, direct marketing purposes, automated decision-making (such as, for example, credit assessment, risk management, insurance underwriting or transaction monitoring to counter fraud) are a few examples of the purposes for which profiling is used by data controllers.

Profiling activities of special categories of personal data are allowed only when the data subject has given explicit consent for the processing of that personal data. Profiling activities requiring the **obtaining of consent are a common practice in the healthcare and biotechnology sectors**.

Poland

Business activity based on big data and profiling is considered a challenge for companies. Such activities require careful implementation of data processing principles, such as privacy by design and by default. Moreover, anonymisation, pseudonymisation and encryption methods should also be applied. High costs of implementation and some misunderstandings regarding the concepts of privacy by design and privacy by default are considered to be the main barriers with regard to profiling and automated decision-making application.

Profiling is of a concern mostly for the financial sector (banks, leasing companies, insurers, etc) and telecommunications providers. Entities from the financial industry apply large-scale profiling, e.g. for credit scoring or marketing purposes.

GDPR requirements also affect significantly the e-commerce industry and marketing activities, where profiling has been widely used. Entities here were forced to verify their processes of client segmentation in order to comply with new requirements.

Romania

There are no derogatory provisions, guidelines or best practices at the level of the Romanian market with respect to what is referred to as qualified profiling. However, there is only one exception to this provided within Law 190/2018, which mentions that the **processing of genetic, biometric and/or health data for the purposes of creating profiles of the individual is permitted only based on the express consent of the individual or if there are distinct legal grounds** allowing for such processing.

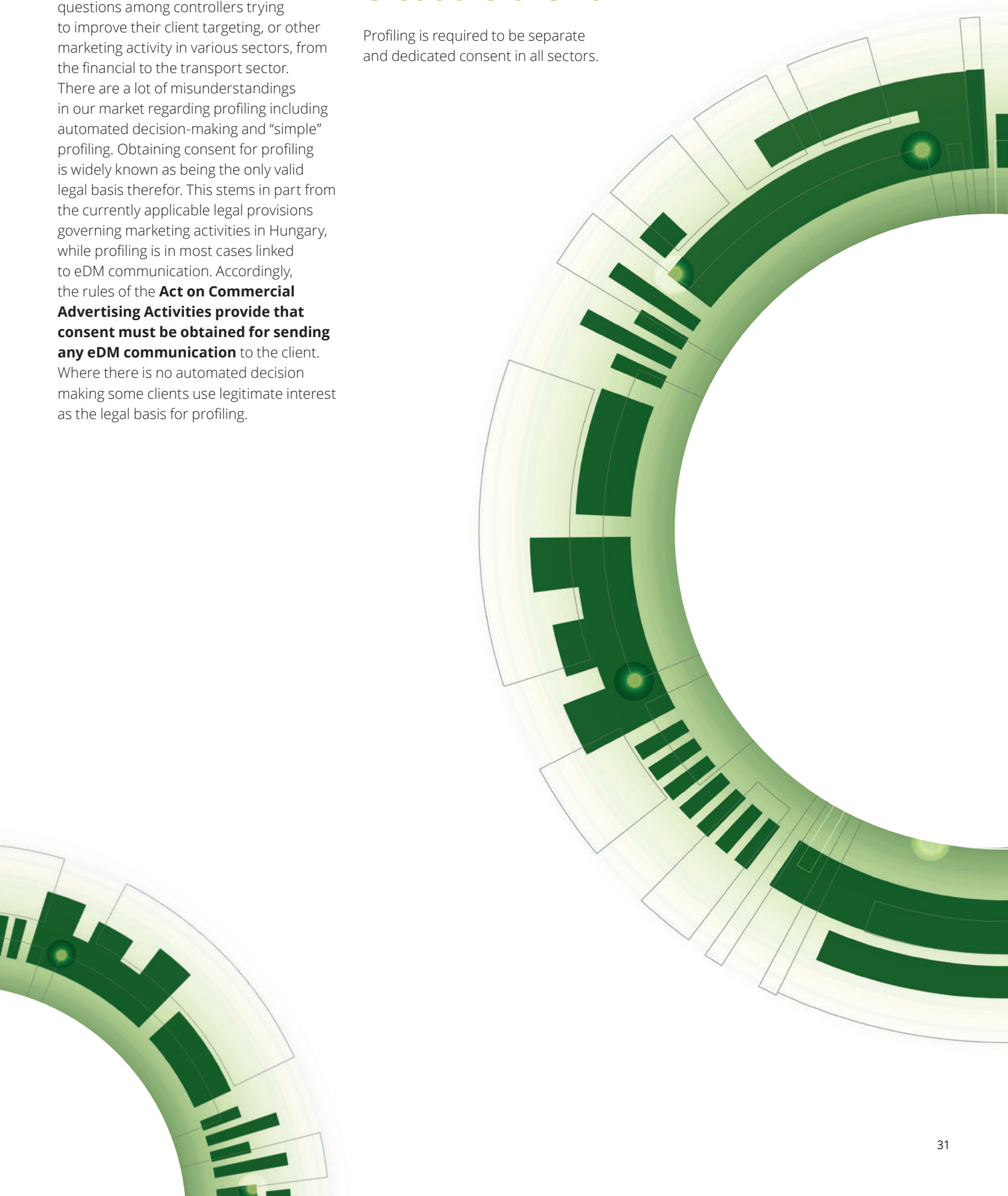
In this respect, companies request the assistance of consultants in drafting of profiling policies that would help employees performing profiling activities for various purposes (e.g. marketing, product development or other business-related purposes) to comply with the provisions of the GDPR and determine when they are in the position of performing intrusive or qualified profiling. Consequently, such profiling policies would also reflect the procedure to be followed by such employees in case a qualified profiling activity is performed – in terms of legal grounds and transparency mechanisms, amongst others.

Hungary

The question of profiling raises numerous questions among controllers trying to improve their client targeting, or other marketing activity in various sectors, from the financial to the transport sector. There are a lot of misunderstandings in our market regarding profiling including automated decision-making and "simple" profiling. Obtaining consent for profiling is widely known as being the only valid legal basis therefor. This stems in part from the currently applicable legal provisions governing marketing activities in Hungary, while profiling is in most cases linked to eDM communication. Accordingly, the rules of the **Act on Commercial Advertising Activities provide that consent must be obtained for sending any eDM communication** to the client. Where there is no automated decision making some clients use legitimate interest as the legal basis for profiling.

Croatia/Slovenia

Profiling is required to be separate and dedicated consent in all sectors.



Renewal of consents and privacy notices

Bulgaria

The controllers have renewed 'old' consents where necessary. They have also satisfied their informational obligation, mainly by serving privacy notices to data subjects as appropriate. For these purposes data controllers use various means: e-mails, hard copies served at the controller's office, website, traditional mail, etc.

The Czech Republic

Generally speaking, the market here has experienced a major wave of consent recollection activities by controllers, as well as notifications regarding amendments to privacy policies, during Q2 2018.

The means of communication used for the above-mentioned activities vary broadly, mainly depending on the standard means of communication with the respective category of data subjects (e.g. in the case of electronic data basis it is sent via e-mail, whereas in case of blue-collar employees a paper version of privacy policy could be handed over in person).

In connection with the issue of excessive usage of consents, some companies have gone through a process of consent renewal, which seemed unnecessary, or which involved an an appropriate approach (e.g. threatening to cancel users' accounts).

Latvia

- It depends on each controller, not all companies decided to renew the consents. However, many companies decided to renew consents before May 2018, and as a result data subjects in Latvia received many e-mail notifications.
- A lot of shops asked customers to renew loyalty cards or sign additional papers, for example when they visited the shop, confirming that the initially provided personal data was still correct.

Slovakia

This depends significantly on the type of business/sector in which a given company is conducting the business and on the type of processing operation for which consent has been used or is being used. Some companies have decided to carry out 're-consenting' (where such operation has been feasible), some have decided to approach the obtaining of the consents gradually through future communication with their clients, and others have decided to look for another, more suitable, legal basis for the processing operations which they previously based on consent.

As regards the provision of the information pursuant to Art. 13 and 14 of the GDPR, the practice here differs as well. Most companies have favoured the option to publish such information on their website, while others provide such information as a part of their e-mail communication, in cases where necessary and feasible. There have also been some companies that have decided to provide data subjects with the necessary information in hard copy, e.g. via post sent to the address of data subjects, in cases possible.

Lithuania

The majority of controllers have renewed 'old' consents and repeated/supplemented the informational obligation in order to comply with the requirements of the GDPR. The market experienced a "major wave" of consent recollection activities of the controllers, as well as notifications regarding amendments to the privacy policies, in May 2018, right before the GDPR came into effect.

The most common means used to do that was e-mail and in some cases via website, telephone or in person.

Poland

In general, controllers opted for sending entirely new information clauses prepared in accordance with the GDPR. Many of these clauses were sent via e-mail (especially by banks, telecommunications providers and energy companies) or in written form. Additionally, clauses are also available on data controllers' websites, including in a form of pop-ups. Most data controllers also needed to refresh the consents they had in place before the GDPR came into force as those did not meet the minimum requirements set out in the applicable regulations and in the WP29 opinion

Romania

As a general observation, the practice of the market participants was to renew the previously obtained consents, as those were generally not considered to be valid under the new GDPR provisions (i.e. in terms of having been granted freely, specific, or not having been stored for accountability purposes). In most cases the new consents are obtained through e-mail and SMS messages. In this respect the most common observation has been that the individuals did not renew their consents, either ignoring the sent e-mail/ SMS or refusing to agree to receiving promotional materials, etc.

As far as privacy notices based on Art. 13 and 14 of the GDPR are concerned, the majority of Romanian companies had not in most cases sent such notices prior to the GDPR becoming effective. Most often such privacy notices were included in what were described as "Confidentiality Policies", or in the data-protection-related chapter in the terms and conditions for the given services/product. As such, once the GDPR became effective these companies sent privacy notices to their employees, customers and business partners, this being one of the easiest measures to be taken in order to comply with the newly applicable regulations. These privacy notices are generally sent to the given data subject as an annex to the contract that the company has with that data subject and, in some cases, informing notices are even made public on the company's website.

Hungary

Starting on 25 May 2018 a huge wave of e-mails deluged Internet users, either asking them to give/confirm their consents or to provide them the infamous information that "we have updated our privacy policy".

In order to comply with the new requirements and best practices, companies offering information technology services tend to provide such information to their customers via e-mail and on their websites. Sending information or consent requests via post is not common and is subject to special rules (sending DM materials by post does not require consent under particular conditions).

In Hungary particular elements (e.g. it is necessary to inform the data subject that if he/she withdraws his/her consent, the data processing remains lawful for the period preceding the date of withdrawal) of proper consent had not been required prior to 25 May, thus those data controllers which did not have this information in their old consent forms had to re-request consent. Major data controllers decided to refresh consents due to the fact that their processing activities had to be specified in a more detailed manner, which previous were covered only with one consent. This required re-aligning their actual processes used for collecting consents and led them to a more consistent and conscious data controlling that supports a wide range of options for targeting their clients, so as to enhance the efficiency of their campaigns.

Croatia/Slovenia

Actions have been taken to renew 'old' consents by many companies on the market, in particular banks and firms from the automotive sector.

Summary

With regard to the main challenges identified in this report, the complexity of issues related to personal data protection mechanisms, especially in big organisations, is of particular noteworthiness. The implementation of the GDPR often requires the involvement of different functions within companies, not only lawyers and privacy specialists, which may create challenges in terms of familiarising staff with the new regulatory framework. As the GDPR is a relatively new regulation, the problem of misinterpretation of its provisions may also be encountered. One of the examples of that is over-reliance on consent as the legal basis for personal data processing. Moreover, in many cases determining the roles of different parties with respect to data processing (i.e. controller, processor role or joint controllers) is challenging. In some countries the national data protection authorities are very active (e.g. through issuance of guidelines), which perceived as an important step towards ensuring legal certainty for market participants.

In some countries, provisions regulating profiling create numerous questions, particularly in heavily regulated sectors, such as the financial services sector. Controllers may face challenges when, for example, deciding on the appropriate legal grounds for personal data processing (consent, legitimate interest, etc). Sometimes it may be difficult to decide whether given operations should be deemed 'qualified profiling' and, therefore, be subject to consent collection.

Among the best practices it has been pointed out that some of the controllers also make their privacy notices publicly available. Another step forward may be the introduction of privacy dashboards that will enable data subjects to easily manage the ways in which their personal data is processed. It has been noted that many companies have introduced special security measures, IT tools and processes in order to ensure high levels of data protection. These practices are found to enhance the security and transparency of personal data processing.

Only a few authorities in the countries covered by this report have not yet issued opinions or guidelines related to data protection issues. Most of the relevant authorities actively support GDPR implementation by issuing templates, guidelines and opinions through which they help to interpret provisions of the GDPR. In most cases fines have not been imposed and inspections have not yet been carried out or are only in their initial phases. Only a few actions of national authorities have been noticed in terms of inspections of GDPR compliance. Generally the authorities seem to be focused on explaining the provisions and pointing out to main issues regarding GDPR compliance. This report also shows activeness in the field of preparation, such as awareness events, training sessions and conferences organised by personal data protection authorities.

In almost every Member State covered by this report sectorial initiatives in the field of personal data protection have been started or even have been completed successfully. These initiatives address, in particular, banking and finance, the medical sector and human resources management. In most cases, the initiatives involve the preparation of codes of conduct.

When it comes to local acts supplementing the provisions of the GDPR, not all of the Member States have adopted appropriate regulations yet, although several of those surveyed stress that their national acts have already been proposed. As far as specific regulations are concerned, most of those relate to the organisation of supervisory authorities, their competences, procedural issues, retention periods, and exceptions and derogations for journalistic, artistic and academic purposes.

Most of the national authorities have not yet published final lists of activities subject to obligatory DPIAs; however, in most cases draft lists are currently subject to public consultation or legislative work. In none of the countries covered herein have list of activities exempted from DPIAs been published. In cases where lists concerning DPIAs have been published, activity based on automated-decision making, video surveillance, monitoring of geographical data on a large scale, and processing of special categories of data (e.g. health, biometric and genetic data) were pointed out as being subject to obligatory DPIAs.

For most of the Member States it has been noted that data controllers generally renewed their 'old' consents in accordance with the GDPR. In some cases it has been pointed out that the adopting of a specific approach depends on the industry or controller. The common practice of delivering privacy notices under Art. 13 and 14 of the GDPR via various means of communication has also been observed.

Contacts

Bulgaria

Miglena Micheva
Legal-Manager
Legal
mmicheva@deloittece.com

Czech Republic

Jaroslava Kračúnová
Legal-Partner
Legal
jkracunova@deloittece.com

Hungary

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

Lithuania

Monika Žlabienė
Legal-Manager
Legal
mzlabiene@deloittece.com

Latvia

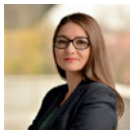
Ivita Samlaja
Managing Associate
Legal
isamlaja@deloittece.com

Poland

Zbigniew Korba
Partner
Legal
zkorba@deloittece.com

Katarzyna Sawicka
Managing Associate
Legal
ksawicka@deloittece.com

Romania



Georgiana Singurel
Partner
Legal
gsingurel@reff-associates.ro

Slovakia

Dagmar Yoder
Legal-Senior Manager
Legal
dyoder@deloittece.com

Croatia/Slovenia

Rado Bekes
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

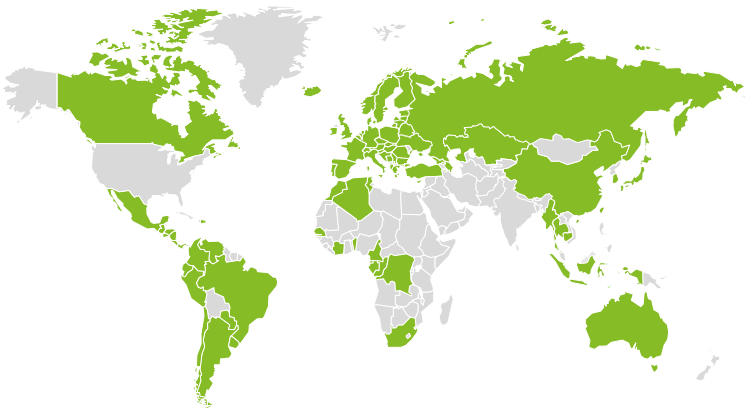
Deloitte Legal Central Europe offers clients numerous fee arrangements tailored for the complexity of the work, such as local or regional preferred rates. This flexibility provides a range of benefits, including:

- 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.