Baker McKenzie.

GDPR National Legislation Survey, 0.3

May 2018

GDPR – National Legislation Survey 0.3 (Update May 2018)

Introduction

This year, as of 25 May 2018, the EU General Data Protection Regulation (GDPR) applies directly in all EU Member States. The GDPR contains 50+ so-called opening clauses allowing EU Member States to put national data protection laws in place to supplement the GDPR. This survey provides an overview of the current legislative activities in terms of national data protection laws supplementing the GDPR of 27 of the 28 EU Member States (Cyprus is excluded). We will update this survey regularly over the coming twelve months.

Update May 2018 – Version 0.3

For this update, we have re-drafted the survey questions considering the recent European-wide developments.

Survey Questions

The survey is broken down into four areas:

1. **Adopted National Data Protection Laws** – Have your local lawmakers **adopted** a statute, act, mandate or other law to supplement the GDPR ("National Data Protection Law") in light of the various opening clauses allowing or requiring EU Member State data protection provisions? If so, please provide a high-level overview of the key provisions, in particular regarding Article 8 and 37(4) GDPR.

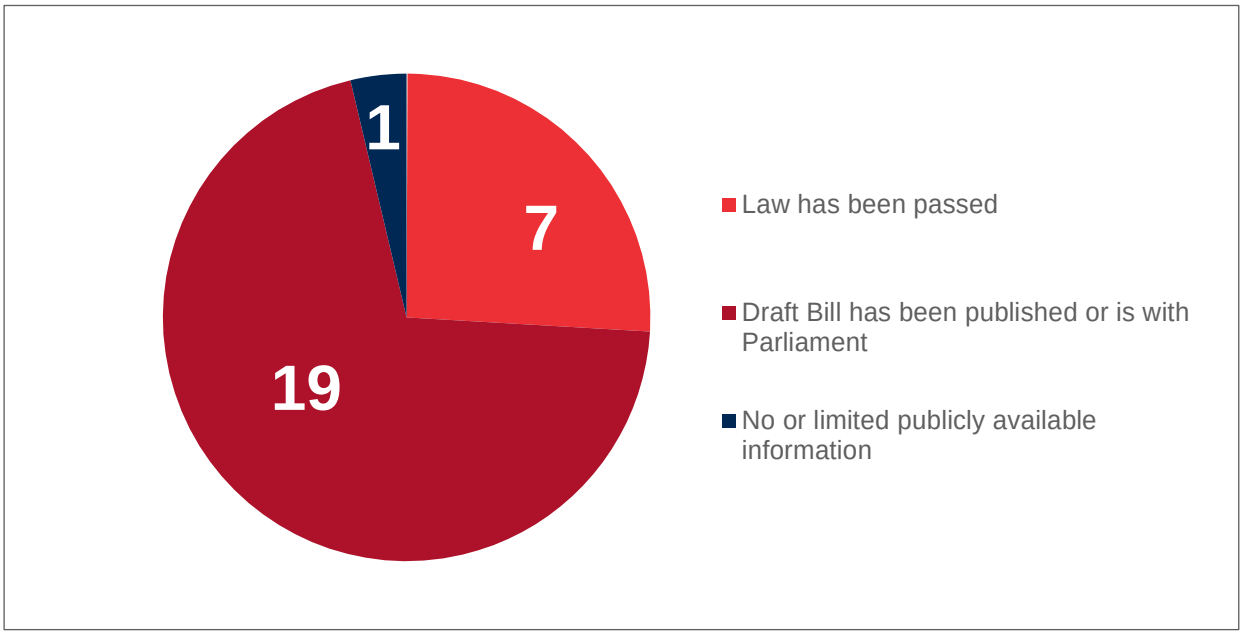
2. **Draft Bills for National Data Protection Laws** – If your answer to Question 1 is no, have your local lawmakers **publicly released** a draft bill for a National Data Protection Law in light of the various opening clauses allowing or requiring EU Member State data protection provisions? If so, please provide a high-level overview of the key provisions and when such draft bill is expected to be adopted.

3. **Other Activities re National Laws** – If your answer to Question 1 and 2 is no, have there been any other declarations, comments or other communication from your local lawmakers regarding potential national data protection laws? If so, please provide some details, in particular roughly when a national data protection law is expected to be adopted.

4. **Key Legal Debates** – What are the most intensely debated issues in respect of the GDPR in your jurisdiction? Are there any other important developments in your jurisdiction, such as guidelines by the authorities?

Findings

Overview over the 27 countries in scope:



- Seven countries have passed acts which came into force on 25 May 2018: **Austria, Croatia**, **Germany, Poland, Slovakia, Sweden and the United Kingdom**.
- Nineteen countries have published a bill, including a bill that is sitting with parliament: **Belgium**, **Bulgaria, Czech Republic**, **Denmark**, **Estonia**, **Finland, France, Greece, Hungary**, **Ireland, Italy**, **Latvia**, **Lithuania**, **Luxembourg, the Netherlands**, Portugal, Romania, Slovenia** and **Spain.**
- One country has not published a bill nor has limited publicly available information on how it will implement the GDPR: **Malta****.

Data Protection Officers

According to Article 37(4), Member States may require the appointment of a data protection officer in scenarios beyond Article 37 (1).

The following Member States have made use of Article 37(4) GDPR in their adopted National Data Protection Laws:

- **Germany** has passed a law which retains the threshold and criteria from previous laws on the appointment of a data protection officer, including for companies with more than nine employees.

The following Member States currently discuss provisions in their national data protection laws in light of Article 37(4) GDPR:

- **Bulgaria**: The draft bill for amendment of the effective Bulgarian Law on Personal Data Protection requires the appointment of a data protection officer if the data controller processes the personal data of more than 10,000 data subjects.
- **France:** The Data Protection Bill of December 2017 would implement a ruling that companies require a data protection officer if certain sensitive data is processed.

**Last update Jan 2018

- **Luxembourg**: The draft bill grants some exemptions from the GDPR's obligations in which a data protection officer could be required.

- **Romania:** The draft bill requires the appointment of a DPO in case of processing of the national identification number.

- **Spain**: The Personal Data Protection Bill contains requirements to appoint a data protection officer in specific circumstances. Furthermore, the Spanish Data Protection Agency has decided to promote a Certification Scheme for data protection officers. This scheme is a certification system that verifies that data protection officers have the professional qualifications and knowledge required to practice the profession. The certification will be granted by certifying entities duly accredited by the National Accreditation Entity.

Prior Authorization Requirements

Current draft bills in France, Luxembourg and the Netherlands seem to indicate that certain limited processing activities will require prior authorization of the local DPA. In France, the current bill requires the CNIL's prior authorization for processing certain sensitive data (e.g., biometric data necessary for identification) and in Luxembourg the draft bill requires the Luxembourg DPA's prior authorization, including for transferring personal data to third countries. The current draft bill in the Netherlands also provides for a prior approval requirement for certain processing activities involving a certain risk and for which prior investigation is required.

Minor Age for Consent

* Unofficial statements or draft bills

Member State	Age Limit	Adopted or Draft Bill
Austria	**14**	**Adopted National Data Protection Law**
Belgium	**Unclear**	**N/A**
Bulgaria	**(16)***	**Draft Bill**
Croatia	**16**	**Adopted National Data Protection Law**
Czech Republic	**(15)***	**Draft Bill**
Denmark	**(13)***	**Draft Bill**
Estonia	**(13)***	**Draft Bill**
Finland	**(13)***	**Draft Bill**
France	**(15/16)***	**Draft Bill**
Germany	**16**	**Adopted National Data Protection Law**
Greece	**(15)***	**Draft Bill**
Hungary	**(16)***	**Draft Bill**

Member State	Age Limit	Adopted or Draft Bill
Ireland	(13)*	Draft Bill
Italy	Unclear	N/A
Latvia	(13)*	Draft Bill
Lithuania	(14)*	Draft Bill
Luxembourg	Unclear	Draft Bill
Malta**	Unclear	N/A
The Netherlands**	(16)*	Draft Bill
Poland	16	Adopted National Data Protection Law
Portugal	(13)*	Draft Bill
Romania	Unclear	Draft Bill
Slovakia	16	Adopted National Data Protection Law
Slovenia	(15)*	Draft Bill
Spain	(13)*	Draft Bill
Sweden	13	Adopted National Data Protection Law
United Kingdom	13	Adopted National Data Protection Law

Baker McKenzie will continue monitoring the progress of all GDPR developments. As there may have been developments since the publication of this survey, please contact Baker McKenzie's Global Privacy Team or the local contributors for the most up-to-date state of play.

Main Editor:

Julia Kaufmann
Partner, Munich
+49 89 5 52 38 242
julia.kaufmann@bakermckenzie.com

Additional Local Contact in Germany:

Holger Lutz
Partner, Frankfurt
+49 69 299 08638
holger.lutz@bakermckenzie.com

Michael Schmidl
Partner, Munich
+49 89 5 52 38 155
michael.schmidl@bakermckenzie.com

A special thanks to our Global Privacy Team, the various contributors and to Kerstin Grimhardt and Olga Bauer in the Baker McKenzie's Munich office for their editorial assistance. If you have any questions, please contact the main editor listed above, your usual privacy contacts or one of our global privacy team members listed below:

GLOBAL PRIVACY TEAM:

North America

Lothar Determann
Partner, Palo Alto
+650 856 5533
lothar.determann@bakermckenzie.com

Michael Egan
Partner, Washington, D.C.
+202 452 7022
michael.egan@bakermckenzie.com

Brian Hengesbaugh
Partner, Chicago
+1 312 861 3077
brian.hengesbaugh
@bakermckenzie.com

Theo Ling
Partner, Toronto
+416 865 6954
theodore.ling@bakermckenzie.com

EMEA

Elisabeth Dehareng
Partner, Brussels
+322 639 3705
elisabeth.dehareng
@bakermckenzie.com

Daniel Fesler
Partner, Brussels
+322 639 3658
daniel.fesler@bakermckenzie.com

Francesca Gaudino
Partner, Milan
+39 0 2762 31452
francesca.gaudino
@bakermckenzie.com

Julia Kaufmann
Partner, Munich
+49 89 5 52 38 242
julia.kaufmann@bakermckenzie.com

Holger Lutz
Partner, Frankfurt
+49 69 299 08638
holger.lutz@bakermckenzie.com

Raul Rubio
Partner, Madrid
+34 91 436 6639
raul.rubio@bakermckenzie.com

Michael Schmidl
Partner, Munich
+49 89 5 52 38 155
michael.schmidl@bakermckenzie.com

Matthias Scholz
Partner, Frankfurt
+49 69 2 99 08 180
Matthias.scholz@bakermckenzie.com

Wouter Seinen
Partner, Amsterdam
+31 20 551 7161
wouter.seinen@bakermckenzie.com

APAC

Anne-Marie Allgrove
Partner, Sydney
+61 2 8922 5274
anne-marie.allgrove
@bakermckenzie.com

Ken Chia
Partner, Singapore
+65 6434 2558
ken.chia@bakermckenzie.com

Kherk Ying Chew
Partner, Kuala Lumpur
+60 3 2298 7933
kherkying.chew@wongpartners.com

Patrick Fair
Partner, Sydney
+61 2 8922 5534
patrick.fair@bakermckenzie.com

Adrian Lawrence
Partner, Sydney
+61 2 8922 5204
adrian.lawrence@bakermckenzie.com

Zhenyu Ruan
Partner, Shanghai
+86 21 6105 8577
zhenyu.ruan@bakermckenzie.com

Paolo Sbuttoni
Partner, Hong Kong
+852 2846 1521
paolo.sbuttoni@bakermckenzie.com

Kensaku Takase
Partner, Tokyo
+81 3 6271 9752
kensaku.takase@bakermckenzie.com

Daisuke Tatsuno
Partner, Tokyo
+81 3 6271 9479
daisuke.tatsuno@bakermckenzie.com

Latin America

Guillermo Cervio
Partner, Buenos Aires
+54 11 4310 2223
guillermo.cervio@bakermckenzie.com

Carolina Pardo
Partner, Bogota
+57 1 634 1559
carolina.pardo@bakermckenzie.com

Flavia Rebello
Partner, Sao Paulo
+55 11 3048 6851
flavia.rebello@trenchrossi.com

Teresa Tovar
Partner, Lima
+51 1 618 8552
teresa.tovar@bakermckenzie.com

Contents

Contributors

Austria	Lukas Feiler, Marisa Schlacher (Baker McKenzie)
Belgium	Elisabeth Dehareng (Baker McKenzie)
Bulgaria	Violette Kunze, Krassimir Stephanov (Djingov, Gouginski, Kyutchukov & Velichkov)
Czech Republic	Milena Hoffmanova (Baker McKenzie)
Croatia	Marija Gregorić, Lovro Klepac (Babic & Partners)
Denmark	Jakob Kristensen, Susanne Stougaard (Bech-Bruun)
Estonia	Merlin Liis, Ants Nõmper, Kairi Kilgi (Ellex Raidla)
Finland	Samuli Simojoki, Louna Taskinen (Borenius Attorneys)
France	Magalie Dansac Le Clerc, Yann Padova (Baker McKenzie)
Germany	Julia Kaufmann (Baker McKenzie)
Greece	George Ballas, Theodore Konstantakopoulos (Ballas, Pelecanos & Associates)
Hungary	Ines Radmilovic, Adam Liber (Baker McKenzie)
Ireland	John Cahir, Chris Stynes (A&L Goodbody)
Italy	Francesca Gaudino, Saverio Puddu (Baker McKenzie)
Latvia	Sarmis Spilbergs, Edvijs Zandars, Liga Merwin (Ellex Klavins)
Lithuania	Jaunius Gumbis, Migle Petkevičienė, Rolandas Valiunas, Tomas Kamblevicius, Kristupas Spirgys (Ellex Valiunas)
Luxembourg	Sybille Briand, Laurent Fessmann (Baker McKenzie)
Malta	Sarah Rutter Giappone (Rutter Giappone Advocates)
Netherlands	Remke Scheepstra, Lotte Ozinga (Baker McKenzie)
Poland	Magdalena Kogut-Czarkowska, Radoslaw Nozykowski, Maciej Niezgoda (Baker McKenzie)
Portugal	Ricardo Henriques (Abreu Advogados)
Romania	Roxana Mitroi, Bogdan Mihai, Iulian Popescu (Musat & Asociatii)
Slovakia	Milena Hoffmanova, Roman Norek (Baker McKenzie)
Slovenia	Markus Bruckmüller, Klara Miletic, Larisa Primozic (Wolf Theiss)
Spain	Raul Rubio, Ignacio Vela (Baker McKenzie)
Sweden	Peder Oxhammar, Jennie Nilsson, Margarita Kozlov (Baker McKenzie)
United Kingdom	Benjamin Slinn, Maura Migliore (Baker McKenzie)

Question 1 – Adopted National Data Protection Laws

Have your local lawmakers adopted a statute, act, mandate or other law to supplement the GDPR in light of the various opening clauses allowing or requiring EU Member State data protection provisions? If so, please provide a high-level overview of the key provisions, in particular regarding Article 8 and 37(4) GDPR.	
Austria	The Data Protection Act ("DPA") 2018 has been passed by the Austrian Parliament, amending the existing DPA 2000 to implement the GDPR and its mandatory opening clauses. The DPA 2018 has been promulgated in Austria's Federal Law Gazette and will enter into force on 25 May 2018.[1] The most important subject matters covered by the DPA 2018 are: 1. The processing of the personal data of a child on the basis that the child's consent is lawful where the child is at least 14 years old (§ 4 para 4 DPA 2018). 2. The DPA 2018 does not provide any protection for data relating to legal persons – however, the constitutional right to data protection under § 1 DPA 2000 remains unchanged and will continue to protect data relating to legal persons (but no fines will exist for any violation of this constitutional right). 3. The processing of personal data relating to criminal convictions and offences or related security measures is authorized according to § 4 para 3 DPA 2018 subject to a prevailing legitimate interest of the controller. The rationale behind the DPA 2018 is to make as few changes as possible to the DPA 2000 and to generally only implement mandatory opening clauses. On 20 April 2018, shortly before the new Data Protection Act was to come into force, the Data Protection Deregulation Act 2018 was passed by the Austrian Parliament, which entails some changes to the new Data Protection Act, of which the most significant is the following: The Data Protection Deregulation Act 2018 limits the right of access of the data subject insofar as this right does not exist if the information of the data subject regarding its personal data by the controller endangers the business or trade secrets of the controller or a third party (§ 4(6) Data Protection Act 2018).
Belgium	No general statute, act, mandate or other law abolishing existing data protection laws and introducing new national provisions to supplement the GDPR has been adopted in Belgium yet, except as detailed below: 1. A new act creating the new Belgian Data Protection Authority in accordance with Article 51 of the GDPR was adopted on 3 December 2017 (and published on 10 January 2018). This act shall enter into force as of 25 May 2018. This act creates and regulates the functioning of the new Belgian Data Protection Authority that will replace the former Belgian Privacy Commission. The new Data Protection Authority shall supervise the processing of personal data on the territory of Belgium and will be capable of controlling (notably via enquiries and inspections) and sanctioning (notably through administrative fines). 2. A new act amending the existing Belgian Act of 21 March 2007 on camera surveillance was adopted on 21 March 2018 (and published on 16 April 2018). This act revises the existing legal framework on the use of surveillance cameras, notably to reflect the modifications brought by the GDPR (including with regard to the notification of data processing activities with the Data Protection Authority and establishment of a record

[1] https://www.parlament.gv.at/PAKT/VHG/XXV/I/I_01761/fnameorig_643605.html

	of processing activities by the controller).
Bulgaria	N/A – no adopted National Data Protection Law yet
Croatia	On 27 April 2018 the Croatian Parliament adopted the national statute implementing the GDPR ("Act"). The Act as adopted by the parliament has not been officially published as yet. Under the publicly available draft bill, as of 25 May 2018, the Act shall completely replace the existing national data protection law and supplement the provisions of GDPR where it allows Member State law to introduce different or additional rules. However, the draft bill which is publicly available contains the following: 1. The bill does not depart from the provisions of the GDPR on the minimum age required for lawful processing based on consent in relation to the offer of information society services to a child. The bill prescribes that such processing shall be lawful if a child as the data subject is at least 16 years of age. 2. The bill expressly prohibits the processing of personal data to assess the prospects of illness and other health aspects related to the data subjects for any conclusion or performance of life insurance agreements or agreements with endowment clauses. Such prohibition may not be derogated from by the data subject's explicit consent. This applies to all data subjects who enter into life insurance agreements and agreements with endowment clauses in Croatian territory if the data controller is located in Croatia or is providing services in Croatia. 3. The bill introduces special rules on processing of biometric data in the public and private sector, and in the context of employment. The processing of biometric data in the private sector is permitted if required by law or necessary for the protection of persons, assets, classified information, business secrets or for an individual and safe identification of users, taking into account whether the interests of data subjects that are contrary to such processing prevail. Biometric data of employees may be processed for the purposes of monitoring working hours and accessing the work premises, if required by law or if such processing is an alternative to another solution for recording working time and the employee has explicitly consented to such processing. Under the bill, video surveillance may be used only for the purpose necessary and justified for the protection of persons and assets, unless interests of data subjects prevail. Special rules apply to video surveillance of employees, public areas, buildings, etc.
Czech Republic	N/A – no adopted National Data Protection Law yet
Denmark	N/A – no adopted National Data Protection Law yet
Estonia	N/A – no adopted National Data Protection Law yet
Finland	N/A – no adopted National Data Protection Law yet
France	N/A – no adopted National Data Protection Law yet
Germany	In May 2017, German lawmakers passed a bill that shall revoke the existing Federal Data Protection Law (*Bundesdatenschutzgesetz* (FDPA)) and enacts a new national data protection law supplementing the GDPR ("Amendment Act"). The Amendment Act had already been passed by the German Parliament (*Bundestag*) in April 2017, and was approved by the Federal Council representing the German states in the national legislative process (*Bundesrat*).[2]

[2] FDPA.new.pdf

	 FDPA new.pdf The German legislature has made extensive use of opening clauses. Some notable provisions of the bill relate to: Protection of data Comprehensive rules on data protection in the employment context have been established. Those rules seemingly build on the current rules under the FDPA as well as the rules and legal opinions that had been formed by German legal literature, courts and DPAs. The Amendment Act specifies the requirement for consent being voluntary and allows for the processing of sensitive personal data of employees for the purposes of an employment relationship if such processing is required to exert rights or comply with duties under employment law, social law or social protection law, and if there is no overriding interest of the data subject. Data protection officer The Amendment Act retains the currently existing thresholds and criteria for the requirement to appoint a DPO. Hence, a company will still be required to appoint a DPO if it permanently employs at least 10 employees where the company is concerned with the automated processing of personal data. Data subject rights Data subject rights, such as right of information, right of access and right to be forgotten, are further restricted. For example, right of access is restricted if the personal data is only stored for compliance with statutory or contractual retention obligations or if the personal data only serves the purpose of data security and data protection control. Right of erasure does not apply if erasure requires an unreasonably great effort due to the specific type of storage. Sensitive data The Amendment Act provides for national law provisions permitting the processing of sensitive data, supplementing Article 9 Sec. 2 (b), (g), (h), (i) and (j) GDPR. Processing of sensitive data is permitted and subject to additional requirements if: (1) the processing is necessary to exercise rights and comply with obligations in the area of social security or social protection laws; (2) for purposes of preventative healthcare, assessment of the working capacity of employees, medical diagnosis, provision of health or social care or treatment, management of health or social care systems and services as well as on the basis of a treatment contract; (3) for reasons of public interest in the area of public health, such as protection against severe cross-border health risks; and (4) for archiving purposes in the public interest, or for scientific or historical research purposes.
Greece	N/A – no adopted National Data Protection Law yet
Hungary	N/A – no adopted National Data Protection Law yet
Ireland	N/A – no adopted National Data Protection Law yet
Italy	N/A – no adopted National Data Protection Law yet
Latvia	N/A – no adopted National Data Protection Law yet

Lithuania	N/A – no adopted National Data Protection Law yet
Luxembourg	N/A – no adopted National Data Protection Law yet
Malta**	N/A – no adopted National Data Protection Law yet
Netherlands**	N/A – no adopted National Data Protection Law yet
Poland	The new Polish Personal Data Protection Act ("PDPA"), which revokes the previous act and serves to supplement and align Polish legislation with GDPR, has been promulgated in the Journal of Laws of the Republic of Poland on 24 May 2018 and entered into force on 25 May 2018. The main subject matters covered by the new PDPA are as follows: 1. Introducing a new data protection authority – the President of the Office for Personal Data Protection ("PUODO") replaced the previous authority i.e., the Inspector General for Personal Data Protection ("GIODO"). In fact, the GIODO office has been renamed PUODO and the GIODO will become the new PUODO and serve in office until the end of its term. 2. Defining the powers and tasks of PUODO as well as procedural rules for audits and proceedings before PUODO. 3. New rules of civil liability for data protection infringements and, accordingly, civil procedure provisions to be applied in such cases before courts. 4. Introducing criminal sanctions for certain violations of GDPR and for obstructing investigations carried out by PUODO. 5. Introducing certification and accreditation mechanisms. 6. Derogations for GDPR applicability in relation to press, literary and artistic activities, as well as processing for purposes of "academic expression." 7. New rules of appointing and notifying DPOs.  ustawa o ochronie danych osobowych.pdf The PDPA also introduced rules regarding the monitoring of employees' both in terms of CCTV and email surveillance. In the PDPA, Polish legislature has **not** made extensive use of opening clauses. However, please note that there is another bill pending (Act on Introducing the PDPA), which will contain provisions aligning various sector-specific laws with the requirements of the GDPR. It is expected that this law will make use of opening clauses for certain industries. Please see also our response to Question 2.
Portugal	N/A – no adopted National Data Protection Law yet
Romania	N/A – no adopted National Data Protection Law yet
Slovakia	The current Data Protection Act was repealed by the DPA and substituted with a new act reflecting the GDPR and including certain derogations therefrom. The act reflects new rules introduced by the GDPR, regulates procedural rules and the status of the authority supervising data protection, as intended by the

GDPR, as well as reflects the decision-making practice of the DPA.

Act Bill Slovakia.rtf

With respect to the opening clauses, the new act establishes the following main derogations or clarifications with respect to the GDPR:

1. Provision of the explicit possibility of a data controller as an employer to provide or disclose personal data of its employees in the extent of: (i) title; (ii) name and surname; (iii) employment, service or functional classification; (iv) personal or employee number; (v) professional formation; (vi) place of work; (vii) telephone number; (viii) fax number; (ix) work email address; and (x) identification data of the employer, if such information is necessary in connection with performance of employment, service or function obligations of the data subject. The provision or disclosure of personal data in such case must not interfere with the seriousness, dignity and safety of the data subject.
2. For the purpose of identification of a natural person, an authorization to use the personal identification number of such person is established, under the condition that such use is necessary to achieve the intended purpose of the processing.
3. Enabling the processing of genetic, biometric and health data on the legal basis of a specific legal regulation or an international treaty to which the Slovak Republic is bound.
4. Anchoring an exception of processing of personal data provided by persons other than the data subject from the requirement of obtaining consent of the concerned data subjects if the personal data is disclosed by such other party only for the purpose of: (i) protection of its rights or legally protected interests; (ii) notification of facts justifying the application of the legal responsibility of the data subject; (iii) where processing of personal data is required under the specific legal regulation or an international treaty to which the Slovak Republic is bound; or (iv) where the processing of personal data is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller.
5. Establishing the authorization of a person close to the deceased person to grant consent to data processing of the deceased person's personal data.
6. Limitation of data controllers' obligations as set out in Articles 12–22 and Article 5 GDPR, and also the establishment of the possibility of a data controller to limit or postpone notification of a personal data breach to the regulatory authorities in cases of: (i) defense or security of the Slovak Republic; (ii) public order; (iii) fulfilling tasks for criminal proceeding purposes; (iv) another important public interest objective of the European Union or the Slovak Republic, in particular important economic or financial interest of the European Union or Slovak Republic, including monetary, budgetary and fiscal matters, public health and social security; (v) preventing violations of ethics in regulated professions and regulated professional activities; (vi) monitoring, inspection or regulatory functions related, even occasionally, to the exercise of official authority in the cases referred to in points (i) to (v); (vii) protection of the independence of the judiciary system and of judicial proceedings; (viii) protection of data subject or rights and freedoms of others; (ix) enforcement of legal claims; or (x) economic mobilization.

Slovenia	N/A – no adopted National Data Protection Law yet

Spain	N/A – no adopted National Data Protection Law yet
Sweden	The Swedish government adopted an act containing supplementary provisions to the EU General Data Protection Regulation (2018:218) (*Lagen med kompletterande bestämmelser till EU:s dataskyddsförordning*,"NDPL") on 24 April 2018. Some notable provisions of the NDPL are: 1. Children's consent The GDPR prescribes 16 as the default age limit for parental consent for processing of personal data in relation to offers of information society services (such as social media, search engines and applications) and contains an opener clause allowing for Member States' legislation to reduce it to 13 at the lowest. Sweden has made use of the possibility to deviate from the default age limit by reducing the aforementioned age limit to 13. For younger children, consent must be given by a custodial parent or the child's consent must be approved by the custodial parent. 2. Sensitive data In addition to the exemptions for processing of special categories of personal data in the GDPR, support is introduced in the Data Protection Act with regard to the necessary processing of personal data in the area of employment law, health and medical care, social care, important public interest, archive activities and statistics activities. Sensitive personal data may be processed under Article 9.2 h of the GDPR, if the processing is necessary due to: (i) preventive healthcare and occupational medicine (ii) assessment of employee working capacity (iii) medical diagnosis (iv) provision of healthcare or treatment (v) social care (vi) management of healthcare services, social care and their systems Processing pursuant to 1–6 above is allowed provided that the duty of confidentiality required under Article 9.3 of the GDPR is fulfilled. 3. Processing of personal data concerning criminal offences Authorities continue to be able to process personal data concerning criminal convictions and offences or coercive measures under criminal law. The Swedish government or an authority appointed by the government may issue explicit support in an act or ordinance or regulations or administrative orders that permits other than the authorities to process such data in certain cases. 4. Personal identity number Absent legitimate consent, personal identity numbers may only be processed where it can be clearly motivated with regard to the processing purposes, the importance of a positive identification or another noteworthy reason. 5. Access to personal data The right to information and access to personal data does not apply to data that is subject to secrecy regulations. Moreover, the right to access to personal data does not apply to personal data contained in running texts that constitute rough drafts or notes, unless the personal data has been transferred to a third

party, the personal data is processed for archiving or statistic purposes or has been processed longer than one year.

6. "Legal obligation" as a basis for processing of personal data

The "legal obligation" basis for processing personal data shall be interpreted as encompassing obligations that follow from a legislative act, other statute, collective agreement or decision issued pursuant to an act or other statute.

7. Duty of confidentiality for DPOs

DPOs in the private sector are expressly bound by a duty of confidentiality under the NDPL. DPOs in the public sector are bound by a duty of confidentiality under the Public Access to Information and Secrecy Act (2009:400).

UK

On 23 May 2018 the UK Data Protection Act 2018 ("DPA") received Royal Assent and the majority of provisions of the DPA came into force on 25 May 2018.

The DPA:

(i) repeals and replaces the UK Data Protection Act 1998

(ii) supplements the GDPR by including certain derogations and options from the GDPR which are left to the authority of individual EU Member States

(iii) extends GDPR standards (with some adjustments) to data processing that does not fall within EU law (i.e., processing in areas which are exclusively regulated under domestic law)

(iv) implements the EU Law Enforcement Directive (regarding data processing for criminal law enforcement purposes)

(v) establishes data protection standards for data processing by intelligence services for national security purposes

Key aspects of the DPA are:

1. The conditions for processing sensitive and criminal data provided in the Data Protection Act 1998 are replicated in the DPA, although under certain circumstances there is an additional requirement that the data controller must have in place an appropriate policy document to establish the procedures for complying with the data protection principles and rules for data retention and deletion.
2. Most of the exceptions to data subject rights which were provided in the Data Protection Act 1998, for example, processing for crime or taxation purposes, are repeated in equal or similar terms.
3. The minimum age for minors to consent to data processing in relation to information society services is set at 13.
4. The safeguards for automated decision-making, such as profiling, which were required in the Data Protection Act 1998 have been carried over to the DPA.
5. Conditions for processing data for research, statistics or archiving purposes are similar to those set out in the Data Protection Act 1998.
6. The DPA does not provide for additional circumstances requiring organizations to appoint a DPO (additional to the circumstances set out under the GDPR).
7. The DPA sets out similar enforcement powers for the Information Commissioner's Office (ICO) as under the Data Protection Act 1998, which include the power to issue information notices, assessment notices, enforcement notices and penalty notices. Under the DPA, the ICO has the power to issue monetary penalties up to the maximum level set out in the GDPR.
8. The Act does not convert the maximum amount of the GDPR monetary

	penalties from euro to pounds. The monetary penalty will be determined in pounds based on the spot rate of exchange set by the Bank of England on the day the penalty notice is given. 9. In addition to replicating or widening the scope of the criminal offenses which were previously contained in the Data Protection Act 1998, the DPA also introduces two new criminal offenses concerning unlawful data processing, namely (i) knowingly or recklessly re-identifying anonymized data; and (ii) altering data to prevent its disclosure following a data subject access request. 10. The Secretary of State may make future regulations to require data controllers to (i) pay a charge to the ICO and (ii) provide information to the ICO for the determination and collection of the charge, which will continue to fund the ICO's activities. As long as the UK continues to be an EU Member State, the GDPR and the DPA together form the statutory framework for UK data protection law. The government's stated intention is to maintain the GDPR provisions following the UK's exit from the EU. To do this, the provisions of the GDPR must be transposed into domestic law by means of the future European Union (Withdrawal) Bill currently before the UK Parliament.

Question 2 – Draft Bills for National Data Protection Laws

If your answer to Question 1 is no, have your local lawmakers publicly released a draft bill for a National Data Protection Law in light of the various opening clauses allowing or requiring EU Member State data protection provisions? If so, please provide a high-level overview of the key provisions and when such draft bill is expected to be adopted.	
Austria	N/A – see response to Question 1
Belgium	No draft bill for a National Data Protection Law introducing new national provisions to supplement the GDPR has been publicly released in Belgium yet.
Bulgaria	A draft bill for the amendment of the effective Bulgarian Law on Personal Data Protection was made available for public discussion on 30 April 2018. The rationale behind the draft bill is the adaptation of the GDPR and the transposition of the Directive 2016/680. The draft bill covers the following subject matters: derogations and specifications with respect to the GDPR (such as criteria for the appointment of a DPO; minor age for consent; launching public registries of DPOs, codes of conduct and certification authorities), the role and the organization of the DPA, regulation of the protection of personal data in processing particularly related to criminal proceedings and the prevention of criminal activities.  Draft Bill Bulgaria.pdf The term for public discussion of the draft bill expires on 30 May 2018. Adoption of the law for the amendment of the effective Bulgarian Law on Personal Data Protection is not expected before mid/end of June 2018.
Croatia	N/A – see response to Question 1
Czech Republic	Currently, the draft of the act is publicly available, together with amending legislation. The primary rationale behind the draft of the new act is the adaptation of the GDPR

and the transposition of the Directive 2016/680, as well as the amendment of the competencies and the organization of the DPA.

The draft of the act covers the following subject matters: derogations and specifications with respect to the GDPR, regulation of protection of personal data in processing particularly related to criminal proceedings and the prevention of criminal activities and in relation to ensuring defense and security of the Czech Republic, the role and the organization of the DPA and the enumeration of offences and corresponding sanctions.

The Czech Ministry of the Interior, in cooperation with the DPA, has proposed a draft of a new Act on Personal Data Processing and other related amendment laws which reflect the GDPR. The draft of the act is currently being discussed by the Chamber of Deputies and will not be adopted prior to the GDPR effectivity date.

The following important areas are worth mentioning:

1. With respect to particularly important cases of processing of personal data in the public interest, the possibility of further processing without the requirement of reviewing the compatibility of the purpose of the original and subsequent data processing is established.
2. A reduction of the age limit for granting online consent to data processing to 15 years.
3. In cases where a data controller carries out processing of personal data necessary to fulfil its legal obligation or a task carried out in the public interest or within the exercise of its authority, such controller may inform data subjects of the processing by disclosing the information in a manner allowing remote access.
4. Introduction of the possibility of the data controller to inform the recipients to whom personal data has been made available of any corrections, limitations or deletions of such personal data also by means of change of the respective personal data in the records, provided that valid contents of such records are regularly made available to the recipient.
5. Exception to the obligation to carry out a data protection impact assessment where certain data processing is regulated by specific legal regulations.
6. Limitation of data controllers' obligations as set out in Articles 12–22 GDPR, and also the establishment of the possibility of the data controller to limit or postpone notification of a personal data breach to the regulatory authorities in cases of: (i) defense or security of the Czech Republic; (ii) public order or internal security; (iii) prevention, search for or detection of criminal activities, prosecution of criminal offences or enforcement of criminal penalties; (iv) another important public interest objective of the European Union or Member State, in particular an important economic or financial interest of the European Union or Member State, including monetary, budgetary and fiscal matters, public health and social security; (v) protection of the independence of the judiciary and of judicial proceedings, or (vi) monitoring, inspection or regulatory functions related, even occasionally, to the exercise of official authority in the cases referred to in points (i) to (v).

Please note that since the proposed draft law has not yet been approved by Czech legislative bodies, it is subject to possible amendments and its wording should be deemed neither final nor binding at this stage.

Draft Bill Czech Republic.pdf

Denmark	In October 2017, the Danish Ministry of Justice proposed a Data Protection Bill. The bill is intended to (i) replace the current Danish Data Protection Act; and (ii) supplement the GDPR by including certain derogations and options from the GDPR which are left to the authority of individual EU Member States. The following key discussion points from the hearing have been included in the proposal: 1. The current rules regarding social security numbers, existing requirements of the disclosure of personal data for marketing purposes and current rules regarding credit rating agencies are upheld. 2. The age limit regarding when children are allowed to independently give consent to the processing of their personal data in connection with the supplying of information services is set to 13. 3. The bill specifically states that the processing of employees' personal data can take place based on consent. The bill is currently going through the parliamentary process.
Estonia	In April 2018 the government of Estonia introduced the draft bill for the new Personal Data Protection Act to parliament. The bill shall replace the current Personal Data Protection Act. The purpose of the bill is to specify and supplement the GDPR and transpose Directive 2016/680. The key provisions of the draft bill (available only in Estonian) include: 1. The rules regarding processing of personal data after the death of the data subject. 2. The right to transfer personal data of the data subject to third persons in case of violation of an obligation by the data subject, and limitations of this right. 3. Rules regarding processing of personal data by law enforcement authorities for the purposes of the prevention, detection, carrying out the procedure and execution of criminal penalties. 4. The provisions regarding that the supervisory authority is to be the Estonian Data Protection Inspectorate and it will be authorized to impose fines in the framework of a misdemeanor procedure. The bill is currently going through the parliamentary process.  Draft Bill of Estonian Personal D
Finland	On 1 March 2018 the Finnish government gave its proposal regarding the adoption of a new Data Protection Act complementing and specifying the regulation contained in the GDPR. The proposed act would be applied parallel to the GDPR. The proposed act would repeal the Personal Data Act (523/1999) and the Act on Data Protection Board and Data Protection Ombudsman (389/1994). The most essential proposals contained in the act are the following: 1. With regard to Article 8 of the GDPR it is proposed that the condition for providing information society services directly to a child is that the child is at least 13 years old (the age limit is set lower than in the GDPR). Children below the age of 13 should obtain parental consent. The data controller is responsible for verifying that valid consent is given. 2. It is proposed that the Data Protection Ombudsman continues to act

as the supervisory authority. The resources of the Ombudsman's office are proposed to be extended and one or more vice ombudsman posts to be established. The current Data Protection Board is proposed to be abolished and instead, an expert board of five members be established in the context of the Ombudsman's office that would adopt opinions regarding the application of the relevant regulations.

3. The Ombudsman could issue conditional fines to businesses, entities and authorities for the reinforcement of its data disclosure orders. The Ombudsman would also be competent to issue administrative fines in accordance with the GDPR. It is proposed that such administrative fines would not be applied to the processing of personal data in the public sector.
4. It is proposed that conduct where a person working for a data controller snoops personal data contrary to the purpose for which the data was collected be criminalized under the Criminal Code (39/1889). The current data protection offense would be repealed from the Criminal Code.
5. Certain exemptions are proposed to be adopted regarding the conditions for the processing of personal data with regard to securing the freedom of expression, for instance, for journalistic purposes. Certain exemptions to the requirements of the GDPR could also be made with regard to scientific and historical research, statistics or archiving, if necessary for research purposes. The exemptions would include the data subject not having inspection rights in such cases. With this regard, the intention in the proposal is that the law would remain as close as possible to the laws currently in force. Also, the processing of data concerning health, sexual behavior and orientation, religion and political views would continue to be possible for scientific and statistical purposes.

The draft bill is currently going through the legislative process in the Finnish Parliament. It has been proposed that the draft bill enter into force on 25 May 2018 at the same time as the GDPR.

Government proposal.pdf

France

The Digital Republic Act (Lemaire Law) of 7 October 2016 already anticipates some provisions of the GDPR, such as:

1. The right to be forgotten.
2. The right for individuals to give instructions relating to the storage, erasure and disclosure of their personal data after their death.
3. Increased sanctioning powers for the CNIL: maximum fines are increased from EUR 150,000 to 3 million in case of data protection infringements.
4. The right to portability.

The Data Protection Bill of December 2017 is transposing and supplementing the GDPR provisions at a local level.

Some notable provisions of the bill relate to:

1. The reinforcement of the CNIL's powers.
2. The reinforcement of the sanctions incurred, which could total EUR 20 million or 4% of consolidated global annual revenues.

3. Certain prior formalities will be maintained "for the processing of the most sensitive data" (biometric data used for identity checks, genetic data, processing using social security number (NIR)). Such processing will also require the appointment of a DPO.

The following resources are available in French only:

1. The Lemaire Law.[3]
2. The parliamentary information report[4] concerning the consequences of the GDPR vis-à-vis the actual regulatory framework regarding data protection.
3. The CNIL annual report.[5]

Data Protection Bill:

- the Data Protection Bill of 14 December 2017[6]
- the Data Protection Bill explanatory memorandum of 14 December 2017[7]
- CNIL's deliberation No. 2017-299 of 30 November 2017 on an opinion related to Data Protection Bill[8]
- opinion of "Conseil d'Etat" on the Data Protection Bill of 11 December 2017[9]
- impact assessment of the Data Protection Bill published by the French government on 13 December 2017[10]
- the current version of the Data Protection Bill of 12 April 2018 submitted for final examination by the National Assembly.[11]

The current version is being discussed by the two chambers of parliament.

It will be reviewed by the French National Assembly on 14 May 2018.

The bill will then potentially be transmitted to the Constitutional Council.

As expected, the Data Protection Bill makes extensive use of opening clauses and maintains, for example, a system of prior authorization for the processing of most sensitive data, e.g., biometric data necessary for identification will be subject to CNIL's prior authorization.

Germany	N/A – see response to Question 1
Greece	On 20 February 2018 a draft bill complementing the GDPR was published and made available for public consultation, which ended on 5 March 2018. The competent legislative committee is now evaluating feedback received during the public consultation procedure; an updated version is expected to be submitted soon to the Greek Parliament for approval. Noteworthy provisions of the draft bill

[3] https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=495DC3C1DF411A0623D70A87FCB381EA.tpdila08v_3?cidTexte=JORFTEXT000033202746&categorieLien=id.

[4] http://www.assemblee-nationale.fr/14/pdf/rap-info/i4544.pdf

[5] https://www.cnil.fr/sites/default/files/atoms/files/cnil-37e_rapport_annuel_2016.pdf

[6] https://www.legifrance.gouv.fr/affichLoiPreparation.do;jsessionid=AD5660270AD9F70B94275AC823321680.tplgfr22s_3?idDocument=JORFDOLE000036195293&type=contenu&id=2&typeLoi=proj&legislature=15

[7] https://www.legifrance.gouv.fr/affichLoiPreparation.do;jsessionid=AD5660270AD9F70B94275AC823321680.tplgfr22s_3?idDocument=JORFDOLE000036195293&type=expose&typeLoi=proj&legislature=15

[8] https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000036195647&fastReqId=180931766&fastPos=1 [9] https://www.legifrance.gouv.fr/Droit-francais/Les-avis-du-Conseil-d-Etat-rendus-sur-les-projets-de-loi/2017/Projet-de-loi-d-adaptation-au-droit-de-l-Union-europeenne-de-la-loi-n-78-17-du-6-janvier-1978-relative-a-l-informatique-aux-fichiers-et-aux-libertes-JUSC1732261L-13-12-2017

[10] http://www.assemblee-nationale.fr/15/pdf/projets/pl0490-ei.pdf

[11] http://www.assemblee-nationale.fr/15/ta/ta0110.asp

include the following:

1. Minor age for consent is set at 15 years.
2. Provisions are introduced for CCTV data processing.
3. Provisions are introduced regarding processing in the context of employment. Employees' heath data can only be collected directly from the employee and only if absolutely necessary for (a) evaluation of an employee's suitability for work; (b) compliance with a legal obligation; (c) establishment of an employee's social security rights. Special rules apply for psychological and psychometric tests and also for the processing of criminal records and genetic data.
4. Provisions are introduced regarding processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
5. Criminal sanctions are being introduced for breach of the GDPR provisions including imprisonment of up to five years and fine up to EUR 300,000. Stricter sanctions are envisaged if breach has an impact on national security.
6. A DPO who violates his/her duty of confidentiality (as envisaged by the draft bill) can be sanctioned with imprisonment of up to five years and fine up to EUR 100,000.

Hungary

On 29 August 2017, the Hungarian Ministry of Justice published the draft Hungarian GDPR Implementation Act for public consultation. The draft legislation adopts a minimalist approach to GDPR implementation, restricting the scope of material changes to existing laws to the bare minimum necessary to comply with the requirements of the GDPR. The main provisions of the draft legislation can be summarized as follows:

1. It extends the provisions of the GDPR to manual processing, even if the personal data is not contained or intended to be contained in a filing system.
2. It does not provide for any special provisions concerning data processing in the context of employment.
3. It maintains the current rules regarding the processing of health data, including the obligation to obtain written consent for such processing.
4. It grants the relatives of a deceased person the ability to exercise the right of erasure and to obtain a restriction on processing upon request within five years following the death.
5. It requires the data controller to review its data processing activities based on Article 6(1)(c) and (e) GDPR every three years, if applicable law does not establish a different time limit for retaining data. The review must be documented and presented to the Hungarian DPA upon its request.
6. It extends the penalty provisions to SMEs by removing the exemption concerning small- and middle-sized undertakings, which to date may receive only a warning (rather than a fine) for their first non-compliance with the law.
7. It no longer requires local filing and/or approval requirements concerning data processed under the GDPR. However, the draft provides that the Hungarian data protection register shall be archived and that the DPA may use the previous filing's details in connection with investigations concerning data processing started before 25 May 2018.

Following the public consultation of the draft Hungarian GDPR Implementation Act, the Hungarian government decided to establish a working group to review the sectoral rules relating to EU data protection reform. The first working group meeting took place in November 2017 and the members were asked to indicate

	possible consistency issues between Hungarian sectoral data privacy laws and the GDPR and to make legislative proposals regarding the review of sectoral data privacy laws in early January 2018. The Ministry of Justice confirmed that the scope of the sectoral rules subject to review is not yet limited. The working group discussed the relevant proposals in February 2018. The Hungarian GDPR Implementation Bill — also including sectoral data privacy rules — is expected to be passed during the spring parliament session.
Ireland	The Irish government has published the Data Protection Bill 2018 but it has not yet been transposed into national law. The Data Protection Bill will give full effect to the GDPR and also to transpose Directive 2016/680.[12] A summary of the bill is also available.[13] A joint committee has carried out pre-legislative scrutiny of the proposed Data Protection Bill.
Italy	The general approach for the implementation of the GDPR reveals the intention to maintain the existing structure of the Italian Privacy Code, currently in place, and adapt it to the provisions of the GDPR. Indeed, the Italian Parliament approved Law No. 163 in October 2017 delegating the government to adopt one or more legislative decrees for the implementation of the GDPR. This law gives the government the authority to modify the Italian Privacy Code (Legislative Decree No. 196/2003), coordinating its text with the GDPR and providing, where appropriate, implementing and integrative measures. The deadline for issuing the implementation law was set at 21 May 2018, but the government recently extended the deadline to 21 August 2018. It is expected that the implementation law is issued by this date. The Italian Data Protection Authority (*Garante per la Protezione dei Dati Personali*) has published documents on its website summarizing the main changes introduced by the GDPR. In particular, said documents provide a description of the data protection officer role, data breach notifications and the right of data portability. The Data Protection Authority also published FAQs on the role of the DPO in the public sector, integrating those already published by the Article 29 Working Party. In addition to Law 163/2017, delegating the government to modify the Privacy Code according to the GDPR (see Question 1), in November 2017, the parliament approved a new law in November 2017 (Law No. 167, published in the Official Journal on 27 November 2017) that modifies the Privacy Code (Legislative Decree No. 196/2003). The bill allows the data controller to nominate as data processors both public and private entities and defines in detail the content and form of the appointment act. In addition, the Privacy Code now also allows, on a case-by-case basis, the re-use of data, even sensitive data (with the only exception being genetic ones), for scientific research or statistical purposes, provided that forms of minimization and anonymization are adopted. With Budget Law No. 205 of December 2017 the Italian Parliament introduced further provisions regarding the implementation of the GDPR: (a) the Italian Data Protection Authority (DPA) will monitor the application of the GDPR and the existence of adequate infrastructures for the interoperability of formats. It will also publish a template privacy notice, guidelines and best practices for the processing operations carried out by data controllers on the ground of legitimate interest using new technologies and automated means; (b) data controllers that carry out processing operations on the ground of legitimate interest using new technologies and automated means are required to make a prior notification to the DPA. The DPA can investigate it and stop processing operations that violate data subjects' rights.
Latvia	The draft of the new Personal Data Processing Law is publicly available and its

[12] http://www.justice.ie/en/JELR/General_Scheme_of_Data_Protection_Bill_(May_2017).pdf/Files/General_Scheme_of_Data_Protection_Bill_(May_2017).pdf

[13] https://www.algoodbody.com/images/uploads/services/EU-Data-Protection/Irish_Government_Published_DP_Bill_2018.pdf

contents are already being discussed. The draft law mostly concerns institutional issues, procedures and judicial relations, focusing on the functions and status of the national data protection authority, data protection officers and other aspects.

Section IX of the draft law lists the main national derogations from the GDPR pursuant to flexibility clauses. For instance, Latvia has chosen the age for minor's consent in relation to information society services under Article 8 GDPR as 13 years. This is due to the fact that many other legislative acts in Latvia already allow children aged 13–16 to decide on a number of things, such as on social services (i.e., rehabilitation, social care and social help services) medical aid, email addresses, as well as being administratively and criminally liable.

The legislator has also relied on Article 85 GDPR to include an exemption from the general rules regarding data processing for journalistic, academic, artistic, literary purposes and freedom of expression.

The draft law also foresees a limitation for data subject access request rights, i.e., that information about the recipients of data can be requested only for the last two years. Furthermore, auditing reports (log files) from systems would need to be stored at least for one year, unless specific laws require otherwise, and if the information requested by data subjects is no longer available, the controller is not required to provide it. As before, when responding to the requests, information should not be provided about law enforcement bodies who have asked/received information in the course of criminal investigations.

Latvia has also opted not to apply the general sanctions regime to public officials. Instead, public officials will be liable for violations in the field of data protection with a fine up to 200 "currency units" (currently one currency unit is EUR 5, thus maximum fine would be EUR 1,000).

Some further changes can still be expected when the draft is reviewed in the next legislative stages. Currently the draft law has been adopted in the first (of three) parliamentary readings.

Lithuania

On 11 April 2018 the Ministry of Justice of the Republic of Lithuania prepared and submitted the third version of the draft of the Law on Legal Protection of Personal Data. The draft of the law follows GDPR requirements closely. It is expected that the draft will be approved by 25 May 2018.

The draft law mostly points to the requirements of the GDPR and only sets forth some specific requirements for:

1. Processing of national identification numbers (as provided for under Article 87 GDPR).
2. Processing of personal data in the context of employment (as provided for under Article 88 GDPR).
3. Conditions applicable to a child's consent in relation to information society services (as provided for under Article 8 of GDPR).
4. Imposing lower administrative fines for public authorities and agencies (as provided for under Article 83 of GDPR).

The draft also details the competence of the local DPA (the State Data Protection Inspectorate of the Republic of Lithuania (Inspectorate)) as well as its powers, tasks and procedure for imposing a fine.

Please note that the draft law may change subject to the results of the consultation and other legislative initiatives which may follow. Taking into consideration that GDPR has already come into force, the third version of the draft law should not be amended.

The Inspectorate has also submitted proposals to amend two Resolutions of the Government of the Republic of Lithuania:

5. Resolution of the Government (20 February 2002, No. 262) Regarding the Reorganization of the State Register of Personal Data Controllers, Approval of its Regulations and of the Procedure of Notification by the Personal Data Controllers of the Processing of Personal Data.
6. Resolution of the Government (25 September 2001, No. 1156) Regarding the structural reform of the State Data Protection Inspectorate, providing authorization, approval of the State Data Protection Inspectorate's regulation and partial amendment of related resolutions of the government.

However, no further actions regarding these resolutions have been made.

The Inspectorate will prepare and approve the following projects on the orders of the Inspectorate's director:

1. Confirmation of the notification of data breach rules.
2. Confirmation of the list of processing operations which are subject to a data protection impact assessment.
3. Confirmation of accreditation criteria.
4. Confirmation of certification criteria.
5. Confirmation of accreditation criteria of certification offices.
6. Confirmation of the standard data protection conditions.

The orders set out above must be coordinated with European Data Protection Board, therefore, these legal acts should come into force only after 25 May 2018 (specific date is still unclear).

Other legislation will be drafted, amended or repealed as needed. No further information relating to opening clauses is available.

Microsoft Word 97 - 2003 Document

Luxembourg

There are three principal draft laws:

1. Luxembourg Draft Law No. 7049 amending the amended Law of 2 August 2002 on the protection of individuals regarding the processing of personal data.

   The main goal of the proposal is to simplify the formalities of prior authorization regarding processing activities for supervision purposes and transfers of personal data to third countries.
   This draft law is still under examination.

Project Bill dated 31 August 2016 amendin

Position of the Luxembourg Conseil d

2. Luxembourg Draft Law No. 7184 establishing the National Commission for Data Protection and the implementation of EU Regulation 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of individuals with regard to processing personal data and the free movement of this data, amending the Law of 25 March 2015 establishing the procedure for processing and the conditions and procedures for the advancement of state officials and repealing the amended Law of 2 August 2002 on the protection of individuals with regard to processing personal data.

In addition, a second draft bill establishing the National Commission for Data Protection and implementing the GDPR was filed in September 2017 by the Ministry of Communication & Media in Luxembourg (Draft Bill No. 7184).

The draft bill confirms and extends the competences of the CNPD, which will notably be empowered to:

i. monitor compliance with the GDPR by any data controller or processor (as well as with the Draft Bill No. 7168 regarding data processing in criminal matters and matters of national security)

ii. have legal standing and initiate judicial proceedings in the interests of the GDPR

iii. require from any data controller or processor all the necessary information to assess their compliance with the GDPR

iv. order a data controller/processor to suspend or stop the processing of personal data

v. impose administrative penalties and sanctions on parties found to have infringed the GDPR (with periodic penalty payments when necessary)

The draft bill also provides for specific provisions that were left to the discretion of Member States:

- The draft bill grants some exemptions from the GDPR's obligations in case of:
  - i. data processing for the purposes of journalism, university research, art or literature (Article 56 of the draft bill)
  - ii. data processing for the purposes of statistics or scientific or historical research, provided that such "limitations" are proportional to the aim pursued and the nature of the data and of the processing is taken into consideration (Article 57 of the draft bill). The counterpart of the exemptions is a long list of additional safeguards that data controllers processing data for statistics or scientific or historical research must put in place, including, as the case may be, designating a DPO and conducting a data protection impact assessment (Article 58 of the draft bill).
- Regarding the processing of sensitive data, including health data, the draft bill confirms that such processing is allowed for relevant medical bodies and healthcare professionals in the framework of their activities, as well as for research bodies (with appropriate safeguards), social security organizations, insurance companies, pension funds, the Medical and Surgical Mutual Fund and other approved organizations. The lawful transfer of sensitive data between these actors is also facilitated.

3. Luxembourg Draft Law No. 7250 implementing, in tax matters, the provisions of EU Regulation 2016/679 of the European Parliament and Council of 27 April 2016 on the protection of individuals regarding the processing of personal data and the free movement of this data and repealing Directive 95/46/CE.

Malta**	Nothing has been announced as the GDPR will be directly applicable in Member States with effect from 25 May 2018.
Netherlands**	In December 2016, the Dutch government published a ministerial draft bill (freely translated as the "Implementation Act regarding the General Data Protection Regulation") on the official government website. A final legislative proposal has not yet been published. The aim of the Implementation Act is to implement the GDPR in a policy-neutral way. To implement the GDPR in Dutch national legislation the draft bill aims to replace the Dutch Personal Data Protection Act (and intends to follow the Dutch Personal Data Protection Act as closely as possible, with two specific exceptions: (a) changes as to how appointments are made at the competent supervisory authority; and (b) processing of biometric data for the sole purpose of identifying an individual will be allowed). With effect from 6 November 2017, in practice organizations no longer need to report the processing of personal data to the Dutch DPA. With the GDPR, the duty to report comes to an end. Until 25 May 2018, organizations may still report personal data processing but the DPA will as, of 6 November 2017, no longer enforce compliance with this duty to report. This significantly reduces the administrative burden. Only in the event of data processing that involves a certain risk and for which prior investigation is required will the duty to report still apply. This means that the DPA will first examine whether the processing meets the requirements of the Dutch Personal Data Protection Act. Only after approval of the DPA can a controller start processing.  Wet en mvt uitvoering verordenin
Poland	Concerning the PDPA law – see response to Question 1. Together with the PDPA, the Ministry of Digitization proposed an Act on Introducing the PDPA, which contains a number of derogations from the GDPR (opening clauses) to be introduced to specific legal acts, as well as detailed rules regarding data processing by certain types of data controllers. According to the proposal, they will apply in the context of data processed (some examples below): 1. For the purposes of national security, e.g., in relation to soldiers' and military data 2. By public schools, libraries, museums and some other educational and cultural institutions and facilities 3. By legal professionals 4. In public archives and various public registries 5. By collective management societies 6. For public statistical information authorities' purposes 7. By various types of public and government authorities, such as tax authorities 8. By hotels (limited exceptions apply) 9. By banks and insurance sector companies (limited exceptions and special permissions apply) 10. By courts, judicial authorities and registries (e.g., the National Criminal Registry) 11. By the National Health Fund in the context of the public healthcare system 12. By employers, in particular regarding the processing of data in relation to employees and applicants

The Committee for European Affairs is in the process of delivering an opinion on the Act on Introducing the PDPA and is to be submitted to the Council of Ministers. It is expected that the bill will be passed into law in fall/winter of 2018.

Portugal

The Council of Ministers recently approved Draft Bill No. 120/XIII that will ensure the implementation of the GDPR in Portugal.[14] This draft bill is still subject to changes as it will have to be approved by the parliament. The first discussion of the draft bill in parliament was held on the 3 May 2018, where it was heavily criticized by several parties.

Some notable provisions of the bill relate to:

1. On a practical note, and certainly aiming to clear a significant backlog, according to the draft bill, all of the notifications and authorization applications pending decision will expire when the draft bill enters into force.
2. In contrast, the draft bill states that all controllers that have an authorization issued pursuant to the current Portuguese Data Protection Law (Law No. 67/98, of 26 October), will be exempt from undertaking a data protection impact assessment.
3. Also with the aim of alleviating the burden of implementation, the draft bill includes the possibility of having a further six months (i.e., until November) to obtain new consent in line with the requirements of the GDPR.
4. According to the draft bill, the National Commission for Data Protection (*Comissão Nacional de Proteção de Dados* (CNPD)) will remain as the supervisory authority for data protection matters.
5. The competent authority for the accreditation of certification bodies for data protection will be the Portuguese Accreditation Institute, I.P. (*Instituto Português de Acreditação, I.P* (IPAC)).
6. Following other countries' example and the opinion of those most actively discussing the matter in Portugal, the draft bill states that in relation to the minimum age for allowing to process children's personal data in the context of an offer of information society services is 13 years old.
7. With respect to portability, the draft bill states that where interoperability of the data is not technically possible, the data subject has the right to demand that the data is delivered to him/her in an open digital format.
8. With regard to the right to erasure (right to be forgotten), the draft bill provides that in cases where there is a data retention period imposed by law, the right to erasure provided for in Article 17 GDPR can only be exercised after that period.
9. The draft bill has also opted to impose some limitations on data processing resulting from CCTV recording, mostly to comply with the existing legal framework set by Law No. 34/2013 of 16 May and guidelines from the Portuguese Data Protection Authority.
10. In respect of data retention periods, the draft bill clarifies that the data retention period shall be (i) the one that is established by law or regulation; or (ii) the period that is necessary for the purpose of the processing. However, it also adds that: 1) where, by the nature and purpose of the processing, it is not possible to establish the data retention period, the retention of the data shall be deemed lawful; and 2) in case the controller or processor is required to prove compliance

[14] https://www.cnpd.pt/bin/decisoes/Par/40_20_2018.pdf

with obligations, they may retain the data until the statute of limitation period defined by law elapses.

11. Some of the more controversial choices have been with respect to data processing in the context of employment, where the draft law, besides clarifying the legal grounds for processing (generally disqualifying consent except for limited circumstances where there is a benefit for the employee), has included some important limitations on: 1) the use of CCTV recordings, as well as on other technological means of remote surveillance (restricting it for criminal proceedings, or for the purposes of establishing disciplinary liability, however, only if carried out within a criminal proceeding); 2) the processing of biometric data of employees (only allowed for the control of attendance and control of access to the premises); 3) the transfer of personal data of employees between companies (only allowing said transfer in cases of occasional transfer of the employee, as far as the transfer of the data is proportional, necessary and appropriate to the objectives to be achieved or of assignment of employees by a company of temporary work, or secondment to another state).
12. With regards to public entities, the draft bill contains detailed indications on the possible options for appointment of a single DPO for different entities.
13. There is also an indication that processing of personal data by public entities for purposes other than those determined by the collection of the data is allowed, provided that processing is carried out in the public interest.
14. The draft bill also contains specific provisions concerning the processing of data in the context of: 1) public procurement proceedings; 2) health databases or centralized registers; 3) archiving purposes in the public interest; 4) scientific or historical research or for statistical purposes – making reference to the principle of data minimization and to the use anonymization or pseudonymization of the data, whenever the purpose of the controller may be achieved with the data in the referred conditions.
15. The draft bill states that technical guidelines for the application of the GDPR to public entities are to be approved by resolution of the Council of Ministers, which has meanwhile been published (Council of Ministers Resolution No. 41/2018) and establishes the minimum compulsory and recommended technical requirements applicable to the IT systems and networks of public entities, which should be adopted until 29 September 2019.
16. With regards to penalties, the draft law defines three different levels of fines, setting minimum amounts depending on the nature of the infringer or size of the company (large enterprises – from EUR 1,000–4,000; SMEs – from EUR 500–2,000; or individuals – from EUR 250–1,000): 1) very serious administrative offense (with a statute of limitation period of three years); 2) serious administrative offense (with a statute of limitation period of two years); 3) minor administrative offense (with a statute of limitation period of one year).
17. Another controversial option was the choice of exempting the application of fines to public entities, although defining that this option should be reviewed within three years, after the entry into force of the draft bill.
18. Finally, the draft bill foresees a list of criminal offenses similar to that which was already included in the previously existing Portuguese Data Protection Law.

Romania

In March 2018, the Romanian Parliament proposed a Data Protection Bill. The Draft Bill is intended to:

1. Replace the current Romanian data protection legislation, namely, Law No. 677/2001 for the protection of persons with respect to the processing of personal data and free circulation of such data ("Law 677/2001")
2. Supplement the GDPR by including certain derogations and options from the GDPR which are left to the authority of individual EU member states

Key discussion points have been included in the proposal, such as:

1. Processing of genetic data, biometric data or health data is forbidden in specific cases. As per Article 3 (1) of Draft Bill, the processing of genetic, biometric or health data for the purpose of achieving an automated decision-making or profiling process is forbidden, except for the processing carried out by or under the control of public authorities within the limits of the powers conferred by law and under the conditions established by the special laws governing these fields, which also provide adequate safeguards for the data subject. The prohibition cannot be lifted by the consent of the data subject.
2. The processing of a national identification number, including the collection or disclosure of documents containing it, for the purposes of the achievement of legitimate interests pursued by the controller or a third party, shall be carried out by the controller establishing the following guarantees:
    i. The implementation of appropriate technical and organizational measures to respect, in particular, the principle of minimizing data and to ensure the security and confidentiality of personal data processing, in accordance with the provisions of Article 32 of the GDPR
    ii. The appointment of a DPO in accordance with Article 8 of the Draft Bill
    iii. Adherence to an approved code of conduct under Article 40 of the GDPR and assuming compliance with its provisions
    iv. Setting retention periods according to the nature of the data and the purpose of the processing, as well as specific deadlines in which personal data must be deleted or revised for deletion
    v. Regular training of the persons who act under the direct authority of the controller or the processor by processing personal data
3. Under the Draft Bill, the monitoring of employees is generally restricted and consequently, allowed in specific cases only. As per Article 5 of Draft Bill, processing of personal data by way of electronic communications monitoring systems/video surveillance systems used at the workplace to achieve the legitimate interests pursued by the employer is permitted only if:
    i. The legitimate interests pursued by the employer concerns activities of great importance, duly justified and prevailing over the interests or rights and liberties of the data subject.
    ii. The employer has notified the employees.
    iii. The employer consulted the trade union or, as the case may be,

	the representatives of the employees before the introduction of the monitoring systems. iv. Other less intrusive forms and modalities to achieve the goal pursued by the employer have not previously proved effective. v. The personal data retention period is proportional to the purpose of the processing, but not more than 30 days, except for situations expressly regulated by the law or duly justified cases. 4. As per Article 12 of Draft Bill, the draft law creates two tiers of maximum fines for authorities and public bodies, depending on the nature of violation. The higher fine is RON 200,000 (about EUR 43,000). The lower fine is RON 100,000 (about EUR 21,500). The Draft Bill is currently going through the parliamentary process. Please note that the date on which the constitutional deadline for debate and final vote of the draft law will be met on 26 June 2018.  Draft Bill Romania.pdf
Slovakia	N/A – see response to Question 1
Slovenia	The latest draft bill was published on 4 April 2018.[15] The draft of the new Personal Data Protection Act covers: 1. Children's consent (age limit is set at 15 years) 2. Processing of personal data about criminal convictions 3. Data processing in the public sector 4. Processing of special categories of personal data 5. Protection of freedom of expression and access to information in relation to the protection of personal data 6. Appointment of a DPO 7. Video surveillance of building entrances, workplaces and public surfaces 8. Biometrical measures 9. Certifications 10. Inspections procedure and competences of the information commissioner The new Personal Data Protection Act is intended to (i) replace the existing Personal Data Protection Act; (ii) regulate certain areas related to opening clauses under the GDPR; and (iii) regulate all data protection matters in a single act. The draft Personal Data Protection Act entered into legislative process at the beginning of April.[16] Due to the resignation of the prime minister and early parliamentary election, it is expected that the new Personal Data Protection Act will be adopted only after 25 May 2018. The new Personal Data Protection Act shall entirely replace its predecessor and implement into Slovenian law Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention,

[15] The draft act is available here: http://www.mp.gov.si/si/zakonodaja_in_dokumenti/predpisi_v_pripravi/

[16] The draft bill is accessible here: https://www.dz-rs.si/wps/portal/Home/deloDZ/zakonodaja/izbranZakonAkt?uid=ACCFF04D8CFAB0FFC1258267003332E3&db=pre_zak&mandat=VII

	investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA. According to the foreword of the draft new Personal Data Protection Act the main purpose of the new Act is to ensure a high level of data protection and alignment of the national law with the new data protection regime under the GDPR. Although consultations were held between the government and the information commissioner during the preparation of the draft act, certain provisions in the latest draft are still not aligned. Soon after the draft act was sent to parliament, the information commissioner submitted its opinion on the latest draft Data Protection Act to the parliament outlining the specific provisions that they consider still not aligned. Therefore, further changes to the draft act may be included into the parliamentary procedure.
Spain	The Personal Data Protection Bill is under discussion in parliament. Relevant changes introduced by the new bill are: 1. Consent for personal data processing must now be affirmative and express (implied consent is excluded). 2. Requirement to appoint a DPO in specific circumstances. 3. Minors above 13 years old can effectively give their consent for the processing of their personal data. 4. Certain special data categories cannot be processed solely on the basis of the express consent of the data subject. 5. The portability right is introduced into Spanish law. 6. Certain kinds of data processing are now presumably based on the legitimate interest of the data controller and, consequently, lawful, such as the processing of contact details and data of individual entrepreneurs, fraud information sharing systems or mail preference systems (Robinson Lists). The political parties have presented their proposed amendments to the bill. Amendments to the whole project have already been debated without success and a total of 369 partial amendments have been submitted and are currently under discussion. Considering how divided the Spanish Parliament is in this legislature, it is difficult to anticipate which of them will be successful. On the other hand, there is the general perception that, given the difficulty in reaching agreements, the approval of the law can be delayed several months, after the deadline of 25 May.
Sweden	N/A – see response to Question 1
UK	N/A – see response to Question 1

Question 3 – Other Activities re National Data Protection Laws

If your answer to Question 1 and 2 is no, have there been any other declarations, comments or other communication from your local lawmakers regarding potential national data protection laws? If so, please provide some details, in particular roughly when a national data protection law is expected to be adopted.	
Austria	N/A – see response to Question 1
Belgium	We understand that a draft bill abolishing existing data protection laws and introducing new national provisions supplementing the GDPR is in preparation and should be introduced before parliament shortly, but no information is currently

	available as to when the draft bill will be publicly available.
Bulgaria	N/A – see response to Question 2
Croatia	N/A – see response to Question 1
Czech Republic	N/A – see response to Question 2
Denmark	N/A – see response to Question 2
Estonia	N/A – see response to Question 2
Finland	N/A – see response to Question 2
France	N/A – see response to Question 2
Germany	N/A – see response to Question 1
Greece	N/A – see response to Question 2
Hungary	N/A – see response to Question 2
Ireland	N/A – see response to Question 2
Italy	N/A – see response to Question 2
Latvia	N/A – see response to Question 2
Lithuania	N/A – see response to Question 2
Luxembourg	N/A – see response to Question 2
Malta**	No official communication has been issued to date.
Netherlands**	N/A – see response to Question 2
Poland	N/A – see response to Question 2
Portugal	N/A – see response to Question 2
Romania	N/A - see response to Question 2 As already mentioned above, the date on which the constitutional deadline for debate and final vote of the Draft Bill will be 26 June 2018.
Slovakia	N/A – see response to Question 1
Slovenia	N/A – see response to Question 2
Spain	N/A – see response to Question 2
Sweden	N/A – see response to Question 1
UK	N/A – see response to Question 1

Question 4 – Key Legal Debates

What are the most intensely debated issues in respect of the GDPR in your jurisdiction? **Are there any other important developments in your jurisdiction, such as guidelines by the authorities?**	
Austria	The new obligation under the GDPR to appoint a DPO, as the current Austrian Data Protection Act does not provide for the legal figure of a DPO. The DPA 2018 does not use the opening clause concerning the mandatory appointment of a DPO. The obligation to appoint a DPO is limited to the cases specified in the GDPR.
Belgium	The Belgian Data Protection Authority (the Belgian Privacy Commission) is quite active regarding the GDPR and dedicated a new section on its website for the GDPR, which includes (i) practical guidance in 13 steps for businesses to prepare for the GDPR; (ii) FAQs in relation to certain aspects of the GDPR; (iii) a recommendation on data protection impact assessments and a diagram on the need to carry out a data protection impact assessment; (iv) a recommendation on the appointment of a data protection officer; (v) a recommendation on the records of processing activities and a template of record; (vi) a guide to help SMEs prepare for the GDPR, etc. A new section containing a detailed legal analysis of the GDPR should be available soon. We are not aware of any indication from the Belgian legislator in respect of dealing with the above issues (other than the Act of 3 December 2017 creating the new Belgian Data Protection Authority and the Act of 21 March 2018 amending the existing Act on Camera Surveillance mentioned under Question 1).
Bulgaria	The most intensely debated issues in respect of the GDPR relate to: 1. Sanctions on the data controllers for non-compliance 2. The new obligation under the GDPR to appoint a DPO and the requirements under the draft bill for appointment of a DPO in scenarios beyond Article 37 (1) of the GDPR 3. The prohibition for public access to the personal identification number of Bulgarian citizens (*ЕГН*) and the use of such personal identification number as a sole identifier of the data subjects.
Croatia	During public consultation in the process of adoption of the national statute implementing GDPR, certain provisions of the GDPR and its opening clauses, including solutions proposed by Croatian government have been debated more intensely, such as: 1. Exemption of public authorities from liability for administrative fines 2. Definition of a public authority introduced by the new statute 3. Processing of sensitive data, specifically personal data related to criminal convictions and/or proceedings and genetic data processed for conclusion or performance of life insurance policies
Czech Republic	Generally, the most intensely debated issues include application of the rules which have been introduced by the GDPR and their implementation by the parties concerned, in particular, their technical and organizational feasibility.
Denmark	Sanctions against public authorities for non-compliance. A popular topic for discussion is whether public authorities should be fined for not complying with the GDPR. According to the proposed Data Protection Bill dated October 2017, public authorities will not be exempt from fines when in breach of people's data protection

	rights. Both the private-sector and public authorities will therefore be subject to fines in Denmark. However, according to the proposed Data Protection Bill, it is the intention that there will be a lower cap on fines issued to public authorities. Registrations with the Danish Data Protection Agency is another topic of discussion. It has been debated whether the general obligation to register and get a prior permission from the Danish Data Protection Agency before processing data purely about private matters, data about criminal offences, or sensitive data, is to be abolished when the GDPR takes effect. It seems from the draft bill that this general obligation will be abolished in accordance with GDPR Recital 89.
Estonia	There have not yet been key legal debates regarding the GDPR. However, in the public media, the most debated issues concern the increased administrative fines and the new obligations of data controllers and processors. Estonian legislation does provide for administrative fines. By now the amendments to the Estonian Penal Code have been introduced to allow for legal remedies with equivalent effect as administrative fines, as required by the GDPR. The Estonian Data Protection Inspectorate publishes, on an ongoing basis, guidance materials and instructions regarding the GDPR requirements (only available in Estonian).[17] Materials published so far include the following topics: 1) when the appointment of a DPO is required; 2) tasks, knowledge and skills required for data protection officers; 3) what the right to data portability is; 4) breach notifications; 5) registration of processing activities; 6) data protection by design and by default; 7) checklist for consent requirements; and 8) checklist for the requirements of a data protection impact assessment. The Estonian Data Protection Inspectorate recently introduced the method for companies to register their DPO online via the Company Registration Portal. The information about the DPOs of the companies will be publicly available in the Business Register after 25 May 2018.
Finland	During the preparation of the GDPR, Finland made an effort to make sure that the provisions of the GDPR will enable the continuation of biobanking, the compilation of wage statistics and genealogy. Finland wanted to particularly retain the transparency of administration by making sure that the GDPR will not affect the principle of openness and the public's right to access official documents. During the circulation for comments, the proposed government bill for a Finnish Data Protection Act received plenty of feedback (published comments available only in Finnish or Swedish).[18]
France	In June 2016, the CNIL launched a public consultation on the right to data portability, the data protection officer, data protection impact and assessment and certification labels. In November 2016, the CNIL published the results[19] of the June 2016 public consultation. On 10 April 2017, the CNIL issued a press release[20] where it informed that the Article 29 Working Party had adopted "a final version of its first guidelines for professionals on data portability, DPO and lead authority." In addition, on 23 February 2017, the CNIL launched two online public consultations on topics identified by the Article 29 Working Party in its 2017 action plan for the implementation of the GDPR. The first three topics were consent,

[17] http://www.aki.ee/et/eraelu-kaitse/euroopa-andmekaitse-reform

[18] https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=1d738195-b96a-47b8-8a74-6ddda342da60

[19] https://www.cnil.fr/sites/default/files/atoms/files/resultats_de_la_consultation_publique_reglement_0.pdf

[20] https://www.cnil.fr/fr/communique-de-presse-pleniere-du-g29-davril-2017

	profiling and data breach notification. On 23 May 2017, the CNIL issued a press release[21] wherein a summary report[22] was published of the 396 online contributions it received concerning these three topics. As of May 2017, the CNIL has published the following information: 1. Guidelines on data breach notifications[23] on 26 July 2017 2. Updated conditions for obtaining training and governance labels to take into account the requirements of the GDPR on 20 September 2017 3. Guidelines for data processors[24] on 29 September 2017 4. An explanatory note on the Article 29 Working Party's guidelines on Data Privacy Impact Assessment on 18 October 2017 5. An extension for the three main internet browsers (Firefox, Chrome and Opera) that allows users to effectively exercise their right to be forgotten on 31 October 2017 6. An open source software for data privacy impact assessment that facilitates the conduct and formalization of the data privacy impact assessment as required by the GDPR on 22 November 2017 7. An opinion on the Data Protection Bill on 30 November 2017 The CNIL also launched a third online public consultation[25] on 20 September 2017, this time on international transfer of data and on transparency. The CNIL communicated the contributions received.[26] The Lemaire Law already went further than the GDPR by providing a new right for individuals to give instructions relating to the storage, erasure and disclosure of their personal data after their death (reference to Recital 27 GDPR). The Data Protection Bill was presented by the French government on 13 December 2017. This bill enables the practical implementation of the GDPR by updating the Data Protection Act of 6 January 1978. However, the bill needs to be scrutinized in parliament before adoption, which has already taken a few months. Amendments are also expected before final adoption. The Data Protection Bill potentially makes extensive use of opening clauses to maintain more restrictive application of the GDPR obligation to retain control over sensitive data (e.g., social security numbers). With respect to the current version of the bill (dated 16 April 2018), there are several debated issues on which the National Assembly and the Senate have not reached a consensus which are: (i) the effective date of certain provisions regarding class actions; (ii) the age of digital majority; and also (iii) open data of court decisions. The last review of the bill by the parliament is expected at the National Assembly on 14 May 2018.
Germany	The German data protection authorities have issued a wide range of guidance on the GDPR, such as (non-exhaustive list): 1. "Consent in accordance with the GDPR"

[21] https://www.cnil.fr/fr/consentement-profilage-notification-de-violations-synthese-de-la-consultation-sur-le-reglement

[22] https://www.cnil.fr/sites/default/files/atoms/files/syntheseglobale_consultation.pdf

[23] https://www.cnil.fr/fr/notifications-dincidents-de-securite-aux-autorites-de-regulation-comment-sorganiser-et-qui-sadresser

[24] https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-un-guide-pour-accompagner-les-sous-traitants

[25] https://www.cnil.fr/fr/transparence-et-transferts-internationaux-de-donnees-contribuez-aux-nouveaux-themes-de-la

[26] https://www.cnil.fr/fr/consultation-reglement-europeen

	2. "Processing of personal data for advertisement" 3. "Processing in the context of employment" 4. "Joint controllers" 5. "Record of processing activities" 6. "DPO for controllers and processors" 7. Sanctions 8. Data transfer to third countries 9. DPIA 10. Access rights 11. Transparency requirements 12. Right to be forgotten 13. Special categories of data 14. Risks for the rights and freedoms of natural persons State data protection authorities have issued additional guidelines and templates for Records of Processing and Data Processing Agreements. Some state data protection authorities have announced online reporting tools for security breaches and to notify the appointment of a DPO.
Greece	Please see the answer to Question 2. No further guidance on the GDPR or general data privacy related matters have been published by the Greek Data Protection Authority.
Hungary	The most intensely debated topics include data breach notification, DPIA and DPA notifications. Following the publication of the draft GDPR Implementation Act, there was public debate about whether Hungary could maintain the penalty exemption applicable to small- and medium-sized undertakings (SMEs) which to date may receive only a warning (rather than a fine) for their first non-compliance with the law. However, the European Commission confirmed to the Hungarian Ministry of Justice that Hungary may not continue this exemption regarding data privacy violations by SMEs after 25 May 2018.
Ireland	Since the publication of the General Scheme of the Data Protection Bill, the main areas debated have been: (a) the bill's proposal that public authorities are excluded from the administrative fine provisions, save where acting in competition with the private sector; (b) the digital age of consent; and (c) the question of whether legislation should provide for class actions in light of Article 80 GDPR. Following public consultation, the Irish government has agreed to set the digital age of consent at 13 years of age.
Italy	The most debated points concern: 1. The appointment of the data protection officer and, in particular, the technical background (i.e., legal or IT) required to cover this role and the level of the DPO's independence. 2. The notification of a data breach and the formalities required to comply with this obligation. 3. The introduction of an additional requirement of prior notification to the DPA for processing operations carried out on the grounds of legitimate interest and whether this requirement conflicts with the accountability principle. 4. Whether or not the mandatory provisions and guidelines provided by

	the Italian Data Protection Authority prior to the GDPR's implementation (such as provisions on cookies, marketing, profiling, video-surveillance, banking, employees' remote control) will remain in force after May 2018.
Latvia	Given that the fines for violations of personal data processing and enforcement level in Latvia are currently relatively low, data controllers and processors are mostly concerned with the large amounts of possible fines for non-compliance with the GDPR. This has motivated companies to take GDPR more seriously and several have already started compliance procedures, although most of the companies and individuals who will be directly affected by the GDPR have not taken any measures towards complying with all the upcoming requirements set out in the GDPR. There are also ongoing debates and concerns regarding the capacity of the national data protection authority to deal will all its tasks and supervising powers provided by the GDPR. There are several proposals by trade/labor unions, hospitals/university hospitals, credit information bureaus that seek to implement some further derogations specifically applicable to them in their core activities. Since those are merely proposals, it is difficult to predict which ones will be supported in final parliamentary readings. These have not gained much public interest thus far. However, one noteworthy issue is the qualification requirement of DPO – in Latvia currently a person can serve as a DPO only after taking an exam held by a local DPA and initially the draft law wanted to keep the same regime. However, given that the GDPR does not expressly allow Member States to specify further qualification requirements for DPOs and any such requirement could be viewed as a local "barrier," the draft law was supplemented at a later stage to allow a person to serve as a DPO if he or she meets the GDPR requirements or has taken the exam. We understand that there are certain interest groups that would prefer to keep the DPO role only for certified/examined persons and there may still be a debate in final readings whether Latvia could mandatorily impose this examination requirement.
Lithuania	Naturally, the drastically increased fines have raised the most debates in our jurisdiction as businesses are worried about the possibility of fines in a field which is still rather unclear. Currently, the draft Law on Legal Protection of Personal Data only set out provisions establishing lower administrative fines for public authorities and agencies (up to EUR 30,000 if Article 83(4) clauses a–c have been breached and up to EUR 60,000 if Article 83(5) clauses a–e and/or Article 83(6) have been breached). There were also debates on how the new data subject rights introduced by the GDPR, right to data portability and right to be forgotten, will have to be implemented. Areas such as stricter requirements for consent, requirements for a child's consent and the scope of application of the GDPR have been discussed and identified as the most important upcoming changes. The draft of the law provides no indications on how these aspects shall be implemented. In addition, the State Data Protection Inspectorate (Inspectorate), in contributing to the implementation of the GDPR in Lithuania, prepares methodical information, guidelines, etc. for the processing of personal data in enterprises, institutions, organizations and individuals in their professional activity, which would help to prepare for the new legal regulation on personal data protection in practice. For example, the Inspectorate has prepared: 1. Public consultation on DPOs. 2. Twelve steps that should be taken to prepare for the GDPR.

	3. Information, examples and presentations on legislative processes regarding national data protection laws supplementing the GDPR.
Luxembourg	There have not yet been any detailed or official indications or topics. There only is a general statement from the Luxembourg prime minister who confirmed that Luxembourg will welcome and apply the GDPR as an opportunity to increase the protection of customers.
Malta**	The most intensely debated issues are: 1. **The definition of consent:** Consent will now have to be proven by the data controller and will be made "by a statement or by a clear affirmative action" (Article 4(11), Regulation 2016/679). 2. **The right to erasure (right to be forgotten):** Where there is no further legal ground for processing personal data, data subjects may request the removal of their personal data "without undue delay" (Article 17, Regulation 2016/679). Organizations must therefore have the technical capacity and procedures in place to enable the removal of personal data based on a request made under Article 17 of the Regulation. 3. **The increased responsibility of data processors:** The regulation aligns the rights and obligations of the data processor with those of the data controller. In particular, the regulation introduces the concept of "joint and several liability" for damage suffered by the data subject. (Article 82(1), Regulation 2016/679). This means that in the event of a breach, the data subject can pursue either the data controller or processor or both parties. This may create legal uncertainty if not tackled in a back-to-back agreement between the data processor and data controller. 4. **The obligation to notify data protection breaches:** Notification which is currently contained to the telecommunication sector by virtue of the ePrivacy Directive will apply to breaches for processing personal data following 25 May 2018 (Articles 33 and 34, Regulation 2016/679). 5. **Cross-border transfers of personal data outside the EU:** Following the *CJEU Schrems* ***v.*** *Data Protection Commissioner (Ireland)* judgment (6 October 2015) challenging the adequacy of the safe harbor standard contractual clauses, standard contractual clauses such as the EU Privacy Shield are also still debatable. 6. **Privacy Impact Assessments:** These will now be mandatory pursuant to Article 35 of Regulation 2016/679. No official communication has been issued to date.
Netherlands**	Please see the answer to Question 2.
Poland	The Polish Data Protection Authority has issued limited guidance in particular regarding (non-exhaustive list): 1. Record of processing activities (with record template) 2. Understanding of the “risk based approach” 3. DPIA (referring to guidance provided by CNIL) Furthermore in April 2018, the Polish Data Protection Authority published a proposal of the list of data processing activities where a PIA is necessary (black list). The proposal was subject to consultations which closed on 30 April. There is no final list yet. Generally speaking, the proposal follows the criteria which were proposed by Working Party Article 29 in its opinion, with additional criterion which is “trans-border data flows outside of EU.”

Portugal

The most intensely debated issues are as follows:

1. Changes to the structure and organization of the CNPD.
2. Sanctions and their application to public entities.
3. Limitations to processing of HR data.
4. DPO role and requirements.
5. The right to erasure (right to be forgotten).
6. Childs age limit, verification mechanisms and requirements for consent of the parent or legal guardian.

Following the approval by the Council of Ministers of Draft Bill No. 120/XIII, the National Commission for Data Protection (*Comissão Nacional de Proteção de Dados* (CNPD)) was asked to give an opinion on the draft bill.[27]

In the opinion (Opinion No. 20/2018), the CNPD strongly criticizes the wording of the draft bill. In particular, CNPD considers that:

1. The draft bill does not comply with European Union law given that (i) the provisions of the draft bill relate to matters for which the GDPR did not give the Member States autonomy to legislate; (ii) some provisions of the draft bill only replicate what is already foreseen in the GDPR; and (iii) in some cases the provisions of the draft bill are simply contrary to what is stipulated in the GDPR.

   In particular, according to the CNPD's understanding, the draft bill infringes European Union law with regard to the following subjects:

   i. scope of application
   ii. provisions with regard to the CNPD
   iii. the DPO
   iv. portability
   v. duty of secrecy
   vi. retention period
   vii. transfers of personal data

2. The draft law foresees a set of provisions establishing the different legal status for data processing when the controller or the processor are public entities. In particular, the critics focus on the following points:

   i. The fact that processing of personal data by public entities for purposes other than those determined by the collection of the data is allowed, provided that processing is carried out in the public interest.

   ii. The exempting of the application of fines to public entities (although the draft bill defines that this option should be reviewed within three years after the entry into force of the draft bill).

3. With regard to the subjects in which the GDPR instructed Member States to define certain aspects of the data protection regime, the CNPD considers that the proposed wording of the draft bill with regard to these subjects is vague, and does not provide for any specific rules.

4. With regard to penalties, in contrast to what is foreseen in the draft

[27] https://www.cnpd.pt/bin/decisoes/Par/ppl120-XIII.htm

	bill, the CNPD considers that the maximum limits for the fines provided for in the GDPR cannot be limited, nor can minimum limits be set for those fines. 5. Regarding criminal sanctions, the CNPD believes that the regulatory framework provided for in the draft bill should be reviewed, since: i. The criminal sanctions represent a regression in relation to the criminal sanctions currently foreseen in the current Portuguese Data Protection Law (Law No. 67/98, of 26 October). ii. Some of the provisions do not correspond to effective, proportionate and dissuasive sanctions as provided for in Article 84 of the GDPR. Finally, the opinion issued by the CNPD states that in situations where the GDPR allows national legislation to define certain aspects, the provisions of the draft bill should be changed, either because in some situations they are unclear, because the provisions violate principles of data protection, or because they simply do not foresee certain situations that should be included in the draft bill (i.e., processing of data concerning health; personal data of deceased persons; data processing resulting from CCTV recording; data processing in the context of employment).
Romania	According to unofficial information received from representatives of the Romanian National Supervisory Authority for Personal Data Processing (Romanian DPA) ("ANSPDCP"), the most intensely debated aspects are related to (i) the procedure for applying the sanctioning regime; (ii) whether the notification system should be maintained. The Romanian DPA is quite active regarding the GDPR and dedicated a new section on its website for the GDPR, which includes practical guidelines to prepare for the GDPR. The Romanian DPA has published several guidelines on GDPR (e.g., novelty elements brought by GDPR, the GDPR Implementation Guide).
Slovakia	Similar to the legal debates in the Czech Republic, the discussed issues relate to uncertainties arising from missing national legislation which would specify some of the general rules set out in the GDPR. Furthermore, since Slovakia has decided to take an unusual approach and create a completely new act for the transposition of the GDPR, the focal point of the debate revolves around the question of whether the completely new law was necessary since the GDPR applies directly to all Member States. Certain ambiguity may arise with respect to the question of which legal regulation to primarily abide by – the wording of the GDPR or the wording of the new act, or a mixture of both. Nevertheless, the wording of the draft of the act seems in most cases to mimic the wording of the GDPR.
Slovenia	The most debated issues are (i) consent requirements; (ii) profiling and automated decision making; (iii) significantly higher sanctions for breaches; (iv) data breach notifications; (v) legitimate interest; and (vi) personal data processing in the course of employment. Additionally, since it became apparent that the national legislation will not be adopted before 25 May 2018, this raised a lot of discontent in various industries, especially the more regulated industries, such as the banking and insurance sectors.
Spain	The Spanish Data Protection Agency ("SDPA") published a report answering several questions about the legitimate interest as a legal basis for personal data processing. The SDPA used to follow a strict interpretation of this concept, only applying the legitimate interest exception in some circumstances and on a case-by-case basis. This report is relevant because the SDPA shows a different

	interpretation criteria, stating several situations in which personal data processing could be based on the data controller's legitimate interests. This change may reflect the SPDA's future stance for the application of the Personal Data Protection Bill. The SDPA has published several documents providing guidance in the implementation of the GDPR and its interpretation: • Guide to the General Data Protection Regulation for data controllers. • Guide for the fulfillment of the duty to inform. • Guidelines for the drafting of contracts between data controllers and data processors. • Guidance and guarantees in the procedures of anonymization of personal data. • Practical Guide for Risk Analysis. • Practical Guide for Impact Evaluations. The SDPA has decided to promote a Certification Scheme for DPOs. This scheme is a certification system that verifies that DPOs have the professional qualifications and knowledge required to practice the profession. The certifications will be granted by certifying entities duly accredited by ENAC (the national accreditation entity). As previously outlined, Spanish operators are concerned about the legitimate interest acting as a legal basis for the processing of personal data. Its use was very limited in Spanish law before the GDPR and its later local implementation and SDPA was especially strict in its practical application. However, the report published by the SDPA can be seen as an indication of how it is going to proceed in relation to legitimate interest. The SDPA's stance seems to have changed to a more permissive interpretation. In addition, the inclusion in the Personal Data Protection Bill of some cases of presumable legitimate interest reinforces this idea.
Sweden	The most intensely debated issues are how companies should comply with the requirements of the GDPR and if companies will be able to process personal data concerning criminal offences through whistleblowing systems. In addition, a new camera surveillance act has been drafted in light of the GDPR and will enter into force 25 August 2018.
UK	**Debated issues** The major topics currently debated which have an impact on the application of the GDPR in the UK are related to the consequences of the future Brexit. These are: 1. International data transfers from the EU to the UK, following the UK's exit from the EU, and possible adequacy decisions in the future. The issue for the UK will be that other security legislation, for example the Investigatory Powers Act 2016, may mean that an adequacy decision for the UK is challenging, regardless of whether the GDPR is implemented in full. The government has proposed (in August 2017) and recently reiterated (in May 2018) future reciprocal adequacy recognitions with the EU so as to enable free flows of personal data in both directions (from the EU to the UK and vice-versa).[28] 2. The role of the ICO on the European Data Protection Board ("EDPB"). The UK government has recently proposed[29] that the ICO maintains an

[28] UK Government, "Framework for the UK-EU partnership. Data protection," May 2018.

[29] UK Government, "Framework for the UK-EU partnership. Data protection," May 2018.

ongoing role on the EDPB following Brexit so that it can continue coordinating with other data protection authorities in the EU to ensure seamless enforcement of the GDPR standards in the UK, and it can remain part of the one-stop-shop mechanism provided under the GDPR. However, the EU's chief Brexit negotiator, Michel Barnier, has so far rejected this proposal.

3. The meaning of the CJEU's jurisprudence in light of the UK's exit from the EU. There is uncertainty on the weight that UK courts will give to the CJEU's jurisprudence following Brexit, however, it will most likely have persuasive authority. In July 2017, the House of Lords EU Committee stated that "The way that EU institutions such as the new European Data Protection Board and the Court of Justice of the European Union interpret the EU's data protection laws could also affect the UK, albeit indirectly—as demonstrated by the experience of the United States with Safe Harbour. Any changes to EU data protection laws would potentially alter the standards which the UK would need to meet to maintain an adequate level of protection."[30]

Future determinations regarding UK-EU data flows, the role of the ICO and the impact of CJEU's jurisprudence on UK law after Brexit will depend on the outcome of the ongoing Brexit negotiations.

Regulatory guidance

The ICO has been updating its Guide to the GDPR. This is a living document which the ICO expands over time with the addition of new guidance on various GDPR topics. The most recent updates or additions to this guidance concern accountability (including documentation and record of processing), data portability and data protection impact assessments.

The ICO has also issued guidance (which sits alongside the Guide to the GDPR) on:

- Automated decision-making and profiling
- Consent
- Children and the GDPR
- Right to be informed
- Data protection impact assessments
- GDPR contracts and liabilities between controllers and processors

The ICO also issued an Introduction to the Data Protection Bill (before the bill was passed into law) which explains the content and structure of the bill. It is now expected that the ICO will produce detailed guidance on the DPA.

[30] House of Lords, EU Committee, "Brexit: the EU Data Protection Package," July 2017.

Baker McKenzie.

www.bakermckenzie.com

Baker McKenzie helps clients overcome the challenges of competing in the global economy.

We solve complex legal problems across borders and practice areas. Our unique culture, developed over 65 years, enables our 13,000 people to understand local markets and navigate multiple jurisdictions, working together as trusted colleagues and friends to instill confidence in our clients.

Baker & McKenzie International is a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organizations, reference to a "partner" means a person who is a partner or equivalent in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.