Baker McKenzie.

GDPR National Legislation Survey, 4.0

August 2018

GDPR – National Legislation Survey 4.0 (Update August 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 in the 28 EU Member States. We will update this survey regularly over the coming twelve months.

Update August 2018 – Version 4.0

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.

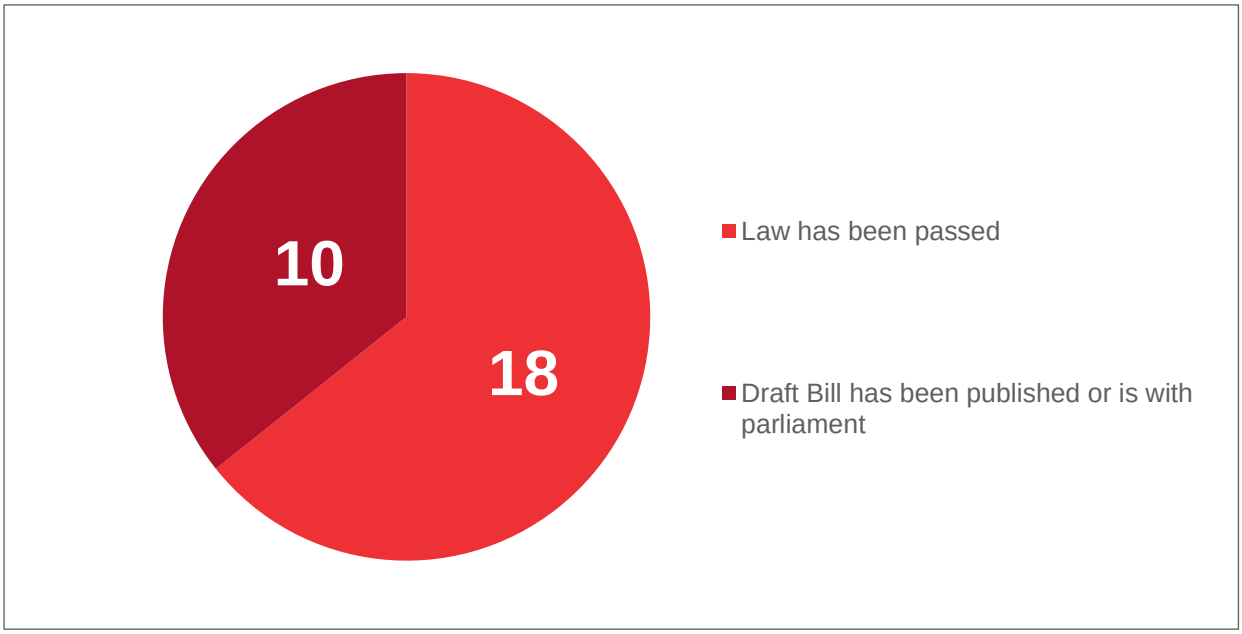
2. **Draft Bills for National Data Protection Laws** – If your answer to Question 1 is no, have your local lawmakers **publicly released** a draft bill for a National Data Protection Law in light of the various opening clauses allowing or requiring EU Member State data protection provisions? If so, please 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 28 countries in scope:



- Eighteen countries have passed National Data Protection Laws supplementing the GDPR: **Austria, Belgium,**[1] **Croatia, Cyprus, Denmark, France, Germany, Hungary, Ireland, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Romania, Slovakia, Sweden** and **the United Kingdom**.

- Ten countries have published a bill, including a bill that is sitting with parliament: **Bulgaria, Czech Republic, Estonia, Finland, Greece, Italy, Latvia, Portugal, Slovenia** and **Spain.**

Data Protection Officers

According to Article 37(4), Member States may require the appointment of a DPO 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 DPO, including for companies with more than nine employees or for companies who are required to carry out a privacy impact assessment pursuant to Article 35 GDPR.

- **Cyprus** has passed a law which empowers the data protection authority to publish a list of circumstances under which the appointment of a DPO is required, beyond Article 37(1).

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

- **France:** The bill on the protection of personal data of 20 June 2018, the French Data Protection Act 2 ("**FDPA 2**"), is intended to bring national law in line with the European Data Protection Package adopted by the European Parliament and the Council on 27 April 2016: the GDPR and the Directive on the "processing operations carried out for the purpose of preventing, detecting,

[1] The Belgian Parliament adopted the new Data Protection Act on 19 July 2018, but it is not yet in force as it still needs to be published.

investigating and prosecuting criminal offenses or carrying out criminal sanctions" (Directive "Police-Justice"). The FDPA 2 does not provide details regarding the DPO with respect to Article 37 GDPR. However, the part of the FDPA 2 which transposes the Directive "Police-Justice" requires the appointment of a DPO by the public authority as a data controller for the processing of personal data for the purpose of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties.

- **Romania:** The new law requires the appointment of a DPO in case of processing of a national identification number for a controller's legitimate interest. According to the law, a national identification number is the number by which a natural person is identified in certain record systems and has a general applicability, such as: personal identification number, serial number and identity card number, passport number, driving license and insurance number for social health.

- **Spain**: The Personal Data Protection Bill contains requirements to appoint a DPO in specific circumstances. Furthermore, the Spanish Data Protection Agency 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. Certification will be granted by certifying entities duly accredited by the National Accreditation Entity.

Prior Authorization/Notification Requirements with the Competent Data Protection Authority

- **France:** The National Data Protection Law in France has abolished the requirement of the previous notification and authorization with the following exceptions: notification/authorization is required (i) for the processing of the national security number (NIR); and (ii) for health data.

- **Cyprus**: The National Data Protection Law in Cyprus requires prior notification of the Data Protection Commissioner (the DPC) if special categories of data shall be transferred to third countries. Prior consultation with the DPC is required (i) if the controller makes use of the right to restrict (in whole or part) the rights in Articles 12, 18,19 or 20 of the GDPR, and/or (ii) if the controller makes use of the right to be exempt from the requirements to communicate a breach to data subjects on the grounds set out in Article 23 (1) GDPR.

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	**13**	**Adopted National Data Protection Law**
Bulgaria	**(14)***	**Draft Bill**
Croatia	**16**	**Adopted National Data Protection Law**
Czech Republic	**(15)***	**Draft Bill**
Cyprus	**14**	**Adopted National Data Protection Law**
Denmark	**13**	**Adopted National Data Protection Law**

Member State	Age Limit	Adopted or Draft Bill
Estonia	Unclear	Draft Bill
Finland	(13)*	Draft Bill
France	15	Adopted National Data Protection Law
Germany	16	Adopted National Data Protection Law
Greece	(15)*	Draft Bill
Hungary	16	Adopted National Data Protection Law
Ireland	16	Adopted National Data Protection Act
Italy	(14)*	Draft Bill
Latvia	(13)*	Draft Bill
Lithuania	14	Adopted National Data Protection Act
Luxembourg	16	Adopted National Data Protection Act
Malta	13	Adopted National Data Protection Act
The Netherlands	16	Adopted National Data Protection Law
Poland	16	Adopted National Data Protection Law
Portugal	(13)*	Draft Bill
Romania	16	Adopted National Data Protection Law
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, in particular to Olga Bauer in Baker McKenzie's Munich office for the 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, Steiner Erik (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)
Cyprus	Anastasios A. Antoniou, Christina McCollum (Antoniou McCollum & Co. LLC)
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)
Netherlands	Remke Scheepstra, Lotte Ozinga Nathalja Doing, Andre Walter (Baker McKenzie)
Poland	Magdalena Kogut-Czarkowska, Radoslaw Nozykowski, Maciej Niezgoda (Baker McKenzie)
Portugal	Ricardo Henriques (Abreu Advogados)
Romania	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 entered into force on 25 May 2018.[2] 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 (Sec. 4(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 Sec. 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 offenses or related security measures is authorized according to Sec. 4(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 – the most significant of which 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 (Sec. 4(6) Data Protection Act 2018).
Belgium	The Belgian Parliament has adopted three acts to supplement the GDPR: Firstly, an act creating the new Belgian Data Protection Authority in accordance with Article 51 GDPR was adopted on 3 December 2017 (and published on 10 January 2018). This act entered into force on 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 supervises the processing of personal data on the territory of Belgium and is capable of controlling (notably via enquiries and inspections) and sanctioning (notably through administrative fines). Secondly, an 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 of processing activities by the controller). Thirdly, the Belgian Act on the protection of natural persons with regard to the processing of personal data was adopted on 19 July 2018 and will come into force on the day of its publication in the Belgian Gazette. This act revokes the existing

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

	Data Protection Act of 8 December 1992. Some notable provisions covered by this new act include: - the minimum age required for lawful processing based on consent in relation to the offer of information society services to a child (13 years old) - particular conditions with regard to the processing of genetic data, biometric data and data concerning health, as well as to the processing of personal data relating to criminal convictions and offenses - restrictions to data subjects' rights in specific circumstances - special rules for the processing of personal data in the public sector, as well as by specific authorities (e.g., police services) - particular provisions with regard to the processing for journalistic purposes and the purposes of academic, artistic or literary expression - provisions applying to the processing of personal data for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes - specific remedies and representation of data subjects - specific sanctions
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**"). As of 25 May 2018, the Act has completely replaced the pre-existing national data protection law and supplements the provisions of GDPR where it allows Member State law to introduce different or additional rules. The Act contains the following: The Act 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 Act prescribes that such processing shall be lawful if a child as the data subject is at least 16 years of age. The Act expressly prohibits the processing of genetic 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. The Act has introduced 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 Act, video surveillance may be used only for necessary and justified purposes 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.

	 National statute implementing GDPR
Czech Republic	N/A – no adopted National Data Protection Law yet
Cyprus	Cyprus enacted the Protection of Natural Persons regarding the Processing of their Personal Data and the Free Movement of such Data, Law 125(I) of 2018 ("**Law**") on 31 July 2018. The Law repeals the Processing of Personal Data (Protection of Individuals) Law 138 (I) 2001 and supplements the GDPR by including certain additional provisions as well as derogations from the GDPR. The key provisions of the Law are summarized below: 1. The processing of personal data by courts of law and parliament is expressly recognized in the Law. 2. The Law sets the minimum age at which minors may lawfully consent to data processing in relation to information society services at 14 (compared to 16 under the GDPR). 3. An express prohibition on the processing of genetic and biometric data for the purposes of life and health insurance is included in the Law. 4. The Law stipulates that a controller can restrict (in whole or part) the rights set out in Articles 12, 18, 19 and 20 GDPR. Where such restrictive measures involve a processor, these measures must be implemented subject to the provisions of Article 28 GDPR. 5. The prior consultation of the Data Protection Commissioner ("**DPC**") is required under the Law for a controller to be exempt (in whole or part) from the requirement to communicate a personal data breach to data subjects (on any of the grounds set out under Article 23(1) GDPR). 6. The Law provides that the DPC may publish a list of processing circumstances in which a DPO must be appointed in addition to those set out under Article 37(1) GDPR. 7. The Law provides that the accreditation of certification bodies in Cyprus will be performed by the Cyprus Organization for the Promotion of Quality. 8. Regarding third country transfers, the Law provides that: (a) Prior to the transfer of special categories of data to a third country or an international organization, a controller or processor must notify the DPC in advance of such intention. (b) The DPC may, on grounds of public policy, impose restrictions on the transfer of special categories of data to a third country or an international organization. (c) The DPC will consult with the European Commission, Council, the lead supervisory authority and other authorities involved prior to imposing any restrictions on an intended transfer of special categories of data to a third country or an international organization (where appropriate safeguards or binding corporate rules have been approved by the European Commission or in the context of the consistency mechanism under Article 63 GDPR). (d) Where transfers of special categories of data to a third country or an international organization are to take place in accordance with the derogations under Article 49, prior consultation with the DPC and the performance of an impact assessment is required. 9. The Law sets out a number of administrative and criminal offenses. In the case of criminal liability where the processor or controller concerned is: (a) an undertaking or a group of undertakings, criminal liability rests

	with the chief executive body of the undertaking or group of undertakings concerned (b) a public authority or body, criminal liability rests with the head of the public authority or body or the person that carries out effective management of the public authority or body
Denmark	The Danish Data Protection Act ("**Act**") entered into force along with the GDPR. The Act has replaced the existing Danish Data Protection Law and supplements the provisions of the GDPR, whereas the most important subject matters of the Act are: 1. The processing of the personal data of a child under 13 years in connection with the offering of information society services is only legal if consent is given or approved by the holder of parental responsibility for the child. 2. Private companies may process information about criminal offenses if (i) the data subject has given explicit consent; or (ii) the processing is necessary for the purpose of safeguarding a legitimate interest that clearly overrides the interests of the data subject. 3. Private companies may process personal identification numbers (*CPR-no.* in Danish) when (i) this follows from the law; (ii) the data subject has given consent; (iii) the processing is carried out solely for scientific or statistical purposes; or (iv) if the other conditions laid down in Article 7 GDPR are satisfied. 4. The Act implements a broad possibility to process personal data in an employment context. Consequently, an employer may process both non-sensitive and sensitive data if (i) the processing is necessary for the purpose of observing and respecting the employment law obligations and rights of the controller or of the data subject as laid down by other law or collective agreements; or (ii) where the processing is necessary to enable the data controller or a third party to pursue a legitimate interest that arises from other law or collective agreements, provided the interests or fundamental rights or freedoms of the data subject are not overridden. Further — and to some extent in contrast to the guidelines from the WP29 group — consent given by the data subject in an employment context in certain situations is a valid legal basis. 5. The Act limits the data subject's rights by possibility of exemption if (i) the data subject's interest in this information is found to be overridden by essential considerations of private interests, including the consideration for the data subject him/herself; or (ii) the data subject's interest in obtaining this information is found to be overridden by essential considerations of public interests, e.g. the prevention, investigation, detection or prosecution of criminal offenses, the protection of the rights and freedoms of the data subject or of others, or the enforcement of civil law claims. 6. The Act determines that the obligation to inform the data subjects in accordance with Article 13(3) and 14(4) GDPR does not apply to public authorities where further processing of personal data for another purpose than the purpose for which it was collected, and the further processing takes place on the basis of rules laid down under Sec. 5(3) of the Act.  The Danish Data Protection Act.pdf Furthermore, the Danish Video Surveillance Act was amended in accordance with the GDPR. The Danish Video Surveillance Act allows economic operators to share picture and sound recordings from video surveillance with other operators for crime prevention purposes.

Estonia	N/A – no adopted National Data Protection Law yet
Finland	N/A – no adopted National Data Protection Law yet
France	On 20 June 2018, the bill on the protection of personal data (the French Data Protection Act 2 or "**FDPA 2**") was officially enacted. To bring national law into line with the GDPR, the government has made the "symbolic" choice not to repeal the founding law on this matter, the French Data Protection Act No. 78-17 of 6 January 1978 ("**FDPA**"). As a result, the FDPA 2 amends the current FDPA. It replaces the logic of prior formalities (notification or prior authorization by the CNIL) by the philosophy introduced by the GDPR of enhanced accountability of stakeholders The most important subject matters covered by the FDPA 2 are: • The notion of sensitive data (Article 8) is broadened: the FDPA 2 repeats the GDPR ban principle on the processing of sensitive data and expands the current scope of this data. The biometric and genetic data will now be regarded as sensitive data. • The prior formalities (Article 11) are mostly abolished: most prior formalities are abolished and will be replaced by the obligation to carry out a privacy impact assessment when the processing operation is likely to pose a high risk to the rights and freedoms of individuals. However, some prior notification and authorization will continue to exist (i) for the processing of the national security number (NIR); and (ii) for heath data. • The definition of the age for "digital majority" (Article 20): the digital majority is established at 15 years. The data controller is then required to deliver the information "in clear and easily accessible language." The national assembly has also developed the conditions of the dual consent mechanism specifying that it should be given jointly by the minor concerned and the legal guardian.
Germany	In May 2017, Germany passed a bill that revoked the existing Federal Data Protection Law (*Bundesdatenschutzgesetz* ("**FDPA**")) and enacted a new national data protection law supplementing the GDPR ("**Amendment Act**").  FDPA new.pdf The German legislature has made extensive use of opening clauses. Some notable provisions of the Amendment Act relate to: 1. Protection of data Comprehensive rules on data protection in an 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 exercise 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. 2. 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 or if a DPIA pursuant to Article 35 GDPR is required.

	3. 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. 4. 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	On 17 July 2018 the Hungarian Parliament adopted Act XXXVIII of 2018, the Hungarian national law supplementing the GDPR, amending Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ("**Amendment**"). The Amendment is in force from 26 July 2018 and it implemented certain important substantive and procedural rules for the application of the GDPR and sanctions for non-compliance. The government also implemented legislation (Act XIII of 2018) designating the Hungarian Data Protection and Freedom of Information Agency (Hungarian DPA) as Hungary's GDPR supervisory authority, which entered into force on 30 June 2018. The Amendment's main provisions are summarized below: 1. Territorial application: the Amendment says that Hungarian data protection law is applicable if either: (i) The controller's main establishment is located in Hungary or the controller's only place of business within the EU is in Hungary. (ii) The controller's main establishment is not located in Hungary or the controller's only place of business within the EU is not in Hungary, but the controller's or its processor(s)'s data processing operation(s) relate to: (a) the offering of goods or services to data subjects located in Hungary, irrespective of whether a payment by the data subject is required; or (b) the monitoring of data subjects' behavior, which occurs in Hungary. 2. Substantive scope: the Amendment extends the GDPR's application to manual data processing, even if the personal data is not contained or intended to be contained in a filing system. 3. Deceased persons: the GDPR applies to living individuals. The Amendment grants the relatives of a deceased person the ability to exercise the right of erasure and to obtain a restriction on processing upon request, made within five years following the death. 4. Data processing by judicial authorities: the Amendment says that data processing activities by courts will be supervised by the courts and not by the Hungarian DPA.

5. Digital age of consent: the age of consent relative to information society services remains 16 years of age under the Amendment.
6. Mandatory data processing: data processing activities based on Articles 6(1)(c) and (e) GDPR must be required by an act of parliament or by a municipality decree. This means in practice that the requirements of government decrees, ministerial decrees and decrees of the National Bank of Hungary or of the Hungarian Media and Info-communication Authority may not be invoked as a mandatory legal basis for data processing under Hungarian law.
7. Statutory review of data processing activities: the Amendment requires the data controller to review data processing activities based on Articles 6(1)(c) and (e) GDPR at least every three years, if applicable law does not establish a specific time limit for retaining the data or for conducting the review of data processing activities. This review must be documented. The related documentation must be retained for 10 years and be presented to the Hungarian DPA upon its request. If the data processing started before 25 May 2018, the controller must perform the first review by 25 May 2021 at the latest.
8. Processing of criminal records data: personal data relating to criminal convictions and offenses may be processed — unless the law provides otherwise — on the legal basis applicable to special categories of personal data. In practice, this means that personal data regarding criminal records (such as a criminal record certificate) may be processed with the data subject's explicit consent or if the data processing is necessary for the establishment, exercise or defense of a legal claim.
9. DPO: the Amendment establishes the confidentiality obligations applicable to a DPO. It does not vary the threshold for appointing a DPO (possible under the opening clause of Article 37(4) GDPR).

    The Amendment also creates a Conference of DPOs, the purpose of which is to keep contact with DPOs and to establish a uniform privacy-related legal practice.
10. Private right of action: the Amendment authorizes individuals to bring private actions against data controllers and processors for GDPR violations. The individual may claim both damages and exemplary damages. Data controllers and processors have the burden of proving their compliance with the legal provisions.
11. Penalty provisions and sanctions: the Hungarian DPA may publish its decision regarding a fine and may identify the controller or the processor fined in the publication if either:

    (i) The decision concerns (a) a wide range of persons; or (b) the activity of a state budget authority.

    (ii) The gravity of the infringement justifies publication of the decision.

    The fine that may be imposed on a state budget authority is capped at a maximum of HUF 20 million (approx. EUR 60,000).
12. DPA registration obligations: the Amendment's ministerial reasoning confirms that no local registration of data processed under the GDPR is required. However, it says that the Hungarian data protection register shall be archived and that the Hungarian DPA may use the previous filing's details in connection with investigations concerning data processing started before 25 May 2018.
13. Certifications: the Amendment defines the framework for supplementing regulations implementing the certification mechanisms under Article 42 GDPR. The Hungarian DPA may perform the certification on the basis of an agreement with the data controller or processor applying for the certification.

Ireland	The Irish Data Protection Act 2018 ("**2018 Act**") was signed into law on 24 May 2018 to supplement the GDPR. It repeals the Data Protection Act 1988, as amended ("**1988 Act**"), except those provisions relating to the processing of personal data for the purposes of national security, defense and international relations of the state. However, the 1988 Act will continue to apply to a complaint by an individual which occurred prior to 25 May 2018. In addition, an investigation that has begun but not completed prior to 25 May 2018 shall be completed in accordance with the 1988 Act. Some notable provisions of the 2018 Act include: • setting the digital age of consent at 16 years • providing that any reference to "child" in the GDPR be taken to be a person under 18 years (other than in regard to Article 8 GDPR) • providing restrictions on individuals' rights and controllers' obligations on the grounds of legal privilege; archiving, scientific or historical research or statistical purposes; freedom of expression and in other specified circumstances for the importance objective of public interest • providing new investigative and enforcement powers for the Data Protection Commission, including enhanced search and seizure powers, the appointment of expert reviewers, the drawing up of investigation reports, examining a witness under oath and conducting oral hearings • establishing a number of criminal offenses punishable by a fine of up to EUR 5,000 and/or 12 months' imprisonment on summary conviction, or up to EUR 250,000 and/or five years' imprisonment on conviction on indictment • providing a lawful basis for the processing of health data for insurance and pension purposes or the mortgaging of property • providing a lawful basis for the processing of data relating to criminal convictions and offenses in specific circumstances, including, where the data subject has provided his/her explicit consent; contractual necessity; for legal proceedings, or to prevent loss/injury or damage to property A summary of the bill is available.[3]
Italy	N/A – no adopted National Data Protection Law yet
Latvia	N/A – no adopted National Data Protection Law yet
Lithuania	On 16 July 2018 the new Law on Legal Data Protection of Personal Data of the Republic of Lithuania came into force. The 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 under Article 87 GDPR). It is forbidden to publish data subject's personal code or to process it for direct marketing purposes. 2. Processing of personal data in the context of employment (as provided under Article 88 GDPR). For example, it is prohibited to process an employee's or candidate's personal data related to criminal convictions or offenses (unless otherwise stated by law). In addition, personal data related to a candidate's qualifications and professional skills may be collected from the candidate's former employer only if the candidate has been informed. However, such personal data of the candidate may be collected from the current employer only if the consent of the candidate has been obtained. 3. Conditions applicable to a child's consent in relation to information society

[3] https://www.algoodbody.com/insights-publications/ireland-passes-data-protection-act-2018

	services (as provided under Article 8 GDPR). In relation to the offer of information society services directly to a child, the processing of the personal data of a child is lawful where the child is at least 14 years old and his/her consent has been obtained. 4. Imposing lower administrative fines for public authorities and agencies (as provided under Article 83 GDPR). The fines are 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. The law 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 administrative fines. However, the Law does not provide any provisions regarding DPOs. The Inspectorate has also submitted proposals to amend two resolutions of the Government of the Republic of Lithuania: 1. Resolution of the Government No. 262 of 20 February 2002 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 2. Resolution of the Government No. 1156 of 25 September 2001 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 approved the following orders of the Inspectorate's director: a) the recommended form of a request for authorization to transfer personal data to third countries or an international organization b) the recommended form of reporting a personal data security breach The Inspectorate plans to prepare and approve the following projects of the orders of the Inspectorate's director in 2018: a) confirmation of the notification of data breach rules b) confirmation of the list of processing operations which are subject to a data protection impact assessment c) confirmation of accreditation criteria d) confirmation of certification criteria e) confirmation of accreditation criteria of certification offices f) confirmation of the standard data protection conditions g) confirmation of rules on conducting investigations carried out by Inspectorate h) confirmation of description of accreditation and the procedure for issuing accreditation certificates i) rules on providing prior consultation
Luxembourg	Draft Law No. 7184 on the organization of the CNPD and implementation of the GDPR became the Law of 1 August 2018 on the Organization of the National Commission for Data Protection and the General Data Protection Regime. The law concerns the creation of the National Commission for Data Protection and the implementation of the GDPR, amending the law of 25 March 2015 establishing the salary system and the conditions and procedures for the advancement of state officials and repealing the amended law of the 2 August 2002 on the protection of individuals with regard to the processing of personal data. Its objective is to adapt Luxembourg law to the new European framework to ensure its full effectiveness for citizens and processors and subcontractors.

	The law 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 law issued from 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 law also provides for specific provisions that were left to the discretion of Member States: ▪ The law 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 law) 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 law). 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 law). ▪ Regarding the processing of sensitive data, including health data, the law 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. In addition, the notification requirement still applies in the context of employee monitoring in an employment relationship as stated in Article 71(4) of the Bill amending Article L. 261-1 of Labor Code. The Draft Law Bill No. 7168 on data protection in criminal matters as well as national security was also adopted on 1 August 2018. This law transposes Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
Malta[4]	The Maltese Data Protection Act 2018 (Chapter 586 of the Laws of Malta) ("**DPA**") was adopted on 28 May 2018. The important subject matters provided by the DPA are: 1. Additional data breach notification requirements: controllers in certain sectors may be required to inform sectoral regulators of certain breaches (for example, financial services entities may be required to report certain breaches

[4] This summary is based on an internet research. Local counsel did not provide updated information.

	to the Malta Financial Services Authority). 2. Language requirements for notices: since Maltese and English are both official languages, providing the information in either of the two languages would be acceptable. 3. Minors: the age of minor consent has been lowered to 13.
Netherlands	The Dutch GDPR Implementation Act which serves to supplement the GDPR was published in the Netherlands' Official Bulletin of Acts and Decrees (Staatsblad 2018 144) on 16 May 2018. The new act covers a number of substantive matters and formalities; it revokes the former Dutch personal data protection act, it re-establishes the institution and powers of the Dutch supervisory authority, and it supplements the GDPR by including certain derogations and options from the GDPR which are left to the discretion of individual EU Member States. Overall, the new act is based on the concept of a 'policy neutral' implementation, meaning that the legislator tried to avoid policy-making where this would lead to a shift from the former data protection regime, and strived for a 'plain vanilla' GDPR roll out. Existing particularities, such as stringent restriction on the use of social security numbers, the treatment of data related to criminal behavior as 'special' personal data and the minimum consent age of 16 remained. The official text, including all national particularities, is available at (Dutch only): https://www.officielebekendmakingen.nl/stb-2018-144.pdf
Poland	The new Polish Personal Data Protection Act ("**PDPA**"), which revokes the previous act and serves to supplement and align Polish legislation with GDPR, was 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	On 17 July 2018 the President of Romania promulgated Law No. 190/2018 ("**Law**") for the implementation of the GDPR with certain relevant provisions penciled into rules and restrictions on the processing of personal data. The most notable provisions of the Law are as follows: 1. The processing of genetic, biometric or health data might only take place when using the explicit consent of the data subject or when it is required by an express legal provision. 2. The processing of data in the context of monitoring the employees may be applied only if the employer used other less intrusive methods which did not render appropriate results in the past. 3. The Law empowers the Romanian Certification Association to set the requirements along with the Romanian Data Protection Authority ("**Authority**") regarding the certification providers. 4. If the public authorities infringe the provision of the GDPR and Law, the Authority shall first notify the aforementioned bodies to impose a mandatory remedy plan. In case of a persistent breach, financial sanctions must be applied. Fines shall not exceed EUR 43,300. On a related matter, private entities shall not benefit from a such privilege, thus, they may be sanctioned directly with fines. Fine limits will be calculated in accordance with GDPR provisions. 5. The Law imposes some derogations from the GDPR regarding the data processing for (i) academic scientific, research or journalistic purposes; (ii) political parties, national minority organizations; and (iii) statistical and archiving purposes. The Law makes no reference or derogation to the minimum age required for lawful processing based on a child's consent. Therefore, according to GDPR provisions, such processing must be lawful if a child, as data subject, is at least 16 years old. In the same line, the Law does not provide additional provisions than those stipulated in the GDPR related to the (i) specific appointment procedure; and (ii) the relevant activity of the DPO.  The implementing Law.pdf
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, processing the personal identification number of such person is lawful under the condition that such processing 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 a 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 a deceased person to grant consent to the 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 EU or the Slovak Republic, in particular, important economic or financial interests of the EU or the 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)–(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	Even though the Spanish Parliament has not yet adopted a national data protection law, the Spanish Data Protection Bill is still under discussion, and the Spanish government has adopted a temporary regulation supplementing certain provisions of the GDPR: provisions regulating the regime on administrative fines. This new regulation (Royal Law-Decree 5/2018 of 27 July on urgent measures for the adaptation of the Spanish law to the EU regulations on data protection) entered into force on 31 July 2018 and will be repealed when the upcoming Spanish Data Protection Bill is finally enacted. The reason why it has been adopted is the existing urgency to supplement several aspects that were not foreseen in the GDPR in relation to the regime on administrative fines. Mainly: • It establishes the limitation periods for each type of infringement: the limitation period for infringements set forth in Article 83(4) GDPR is two years, while the limitation period for infringements set forth in Article 83 (5 and 6) GDPR is three years. • It identifies who may be held liable because of infringements of the GDPR:

	(i) data controllers; (ii) data processors; (iii) representatives; (iv) certification bodies; and (v) accredited bodies monitoring compliance with codes of conduct. • It foresees an in-depth regulation of the cooperation procedures between supervisory authorities with the goal of adapting such cooperation to Spanish law. • It sets forth several provisions regulating the administrative procedures to be conducted by the Spanish Data Protection Authority. It establishes that data processing agreements entered into prior to the 25 May 2018 may remain in force according to their terms. Where a term is indefinite, the DPA will be valid until the 25 May 2022. Nevertheless, any party may require the other to update the agreement in light of Article 28 GDPR.
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 9.2h 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 (i)–(vi) above is allowed provided that the duty of confidentiality required under Article 9.3 GDPR is fulfilled. 3. Processing of personal data concerning criminal offenses Authorities continue to be able to process personal data concerning criminal convictions and offenses 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 for longer than one year. 6. "Legal obligation" 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 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. By means of the European Union (Withdrawal) Act 2018 which was adopted on 26 June 2018, such statutory framework will be retained as UK data protection legislation after the UK leaves the EU.

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	N/A – see response to Question 1
Bulgaria	A final draft bill for the amendment of the effective Bulgarian Law on Personal Data Protection was published on the website of the Bulgarian parliament on 18 July 2018. The rationale behind the draft bill is the adaptation of the GDPR and the transposition of Directive 2016/680. The draft bill covers the following subject matters: derogations and specifications with respect to the GDPR (such as minor age for consent; launching public registries of 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.  Final Draft Bill Bulgaria.pdf Adoption of the law for the amendment of the effective Bulgarian Law on Personal Data Protection is not expected before late autumn of 2018.
Croatia	N/A – see response to Question 1
Czech Republic	The draft of the act is currently 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 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 offenses 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 offenses or enforcement of criminal penalties; (iv) another important public interest objective of the EU or a Member State, in particular an important economic or financial interest of the EU 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
Cyprus	N/A – see response to Question 1
Denmark	N/A – see response to Question 1

Estonia	In April 2018 the government of Estonia introduced the draft bill for the new Personal Data Protection Act to parliament. The bill was supposed to replace the current Personal Data Protection Act and the purpose of the bill was to specify and supplement the GDPR and transpose Directive 2016/680. The bill was withdrawn from the parliament in June 2018. No new draft bill has yet been published.
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 in 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 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 still going through the legislative process in the Finnish Parliament. It has been estimated that the new Data Protection Act would enter into force by the end of this year. However, the timetable is uncertain.  Government proposal.pdf
France	N/A – see response to Question 1
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 include the following: 1. The 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	N/A – see response to Question 1
Ireland	N/A – see response to Question 1
Italy	On 8 August 2018 the Council of Ministers approved the decree of GDPR harmonization. The decree is yet to be published on the Official Gazette, so at the time of this publication, there is no final version. Therefore, our comments refer to the draft provisions, to be confirmed shortly. Among others, some elements worth mentioning are: 1. The current data protection law (Legislative Decree 196/2003, consolidated version) will not be repealed, but instead updated in light of the GDPR. 2. The orders and general guidelines of the Italian privacy authority (*Garante per la protezione dei dati personali*) issued over the years will remain in force, as amended under the GDPR. This entails a robust effort of practitioners and companies in understanding how in practice this harmonization would be interpreted. 3. Criminal sanctions for breach of privacy provisions are confirmed (they were already existing pre-GDPR), with a re-shaping of the specific behaviors that trigger criminal sanctions. 4. The *Garante* will issue specific orders to ease the burden of GDPR implementation for small- and medium-sized companies. 5. For minors, the age to provide valid consent is set at 14 years. 6. An eight-month period is envisaged in which the provisions of the GDPR relating to audits/inspections and consequent sanctioning will somehow be paused. This is not a grace period; instead the rationale is to gradually apply inspection powers and sanctioning rules under the GDPR.
Latvia	The draft of the new Personal Data Processing Law is publicly available and its 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, DPOs 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 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	N/A – see response to Question 1
Luxembourg	N/A – see response to Question 1
Malta	N/A – see response to Question 1
Netherlands	N/A – see response to Question 1
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, for example: • for the purposes of national security, e.g., in relation to soldiers' and military data • by public schools, libraries, museums and some other educational and cultural institutions and facilities • by legal professionals • in public archives and various public registries • by collective management societies • for public statistical information authorities' purposes • by various types of public and government authorities, such as tax authorities • by hotels (limited exceptions apply) • by banks and insurance sector companies (limited exceptions and special

	permissions apply) • by courts, judicial authorities and registries (e.g., the National Criminal Registry) • by the National Health Fund in the context of the public healthcare system • 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.[5] 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 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 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

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

	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 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 – EUR 1,000–4,000; SMEs – EUR 500–2,000; or individuals – 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	N/A – see response to Question 1
Slovakia	N/A – see response to Question 1

Slovenia	The latest draft bill was published on 4 April 2018.[6] The draft of the new Personal Data Protection Act covers: • children's consent (age limit is set at 15 years) • processing of personal data about criminal convictions • data processing in the public sector • processing of special categories of personal data • protection of freedom of expression and access to information in relation to the protection of personal data • appointment of a DPO • video surveillance of building entrances, workplaces and public surfaces • biometrical measures • certifications • 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.[7] 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, investigation, detection or prosecution of criminal offenses 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 recitals 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. A DPO must be appointed 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.

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

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

	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	N/A – see response to Question 1
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
Cyprus	N/A – see response to Question 1
Denmark	N/A – see response to Question 1
Estonia	N/A – see response to Question 2
Finland	N/A – see response to Question 2
France	N/A – see response to Question 1
Germany	N/A – see response to Question 1
Greece	N/A – see response to Question 2
Hungary	Because Hungary did not introduce the required legislative changes before the GDPR became applicable on 25 May 2018, the designation of the Hungarian DPA and the adoption of the Amendment (see response to Question 1) are only part of the GDPR-related legislative developments in Hungary. However, several data protection related issues remained unresolved, because the Amendment did not at all address sectoral data protection laws in Hungary. Therefore, businesses in

	Hungary will continue to encounter inconsistency issues across the range of Hungarian laws that regulate data protection and the Amendment is only best viewed as a next step in this legislative process. A comprehensive data protection legislative reform in Hungary is expected to be adopted during parliament's 2018 fall session. It will need to thoroughly harmonize sector-specific legislation, including the special provisions applicable to: data processing in the context of employment; the processing of health data; and data processing for whistleblowing and for direct marketing purposes.
Ireland	N/A – see response to Question 1
Italy	N/A – see response to Question 1
Latvia	N/A – see response to Question 2
Lithuania	N/A – see response to Question 1
Luxembourg	N/A – see response to Question 1
Malta	N/A – see response to Question 1
Netherlands	N/A – see response to Question 1
Poland	N/A – see response to Question 2
Portugal	N/A – see response to Question 2
Romania	N/A – see response to Question 1
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	One of the most intensely debated issues is 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. The data protection authority established and issued a list (pursuant to Arrticle 35(4), "blacklist") of the kind of processing operations which are subject to the requirement for a data protection impact assessment.
Belgium	The Belgian Data Protection Authority (the former Belgian Privacy Commission) is quite active regarding the GDPR and dedicated an entire 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 DPO; (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. Specific forms are now available on the Belgian DPA's website for the notification of (i) a personal data breach; or (ii) a DPO to the authority. A new section containing a detailed legal analysis of the GDPR should be available soon. The Belgian Data Protection Authority commented on the draft bill on the protection of natural persons with regard to the processing of personal data (see Question 2). which was adopted on 19 July 2018 and is expected to be published soon.
Bulgaria	The most intensely debated issues in respect of the GDPR relate to: • sanctions on the data controllers for non-compliance • protection of professional, commercial and attorney's secrets • the exemption from the general rules regarding data processing for journalistic, academic, artistic, literary purposes and freedom of expression. • the prohibition from 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 • the prohibition from photocopies of identity cards and passports
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: • exemption of public authorities from liability for administrative fines • definition of a public authority introduced by the new statute • 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

	The Croatian Data Protection Authority ("**DPA**") has published GDPR Guidance in addition to the existing guidelines at EU level. GDPR Guidance issued by the Croatian DPA defines the essential terms introduced by the GDPR and provides a summary of GDPR provisions related to legal bases of the processing, data subjects' rights, obligations and rights of data controllers and processors, DPOs, transfers of data to third countries and international organizations and the DPA's enforcement/regulatory powers. The DPA has not published detailed guidelines related to specific areas of the GDPR's application, but only an overview of essential principles contained in the GDPR. In addition, the DPA has prepared and published document templates which may be used by data controllers and processors, such as confidentiality statements and personal data breach notification forms.
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.
Cyprus	Key GDPR issues being debated relate to: • sanctions introduced on data controllers and processors, which involve criminal liability • criminal liability resting with a head of a public authority or the person that carries out effective management of the public authority • uncertainty regarding any additional circumstances in which the data protection authority may require the appointment of a DPO (beyond Article 37(1) GDPR) • prohibition of processing genetic and biometric data for the purposes of health and life insurance The DPC has issued Opinion 1/2018 regarding trade unions in relation to the notification by employers of a statement containing a list of names, salaries and amount of deductions in respect of contributions. The DPC has also confirmed that the following Directives issued under the previous regime are to remain binding until replaced or revoked: • Directive on video surveillance (2004) • Directive on employment relations (2005) • Directive on the use of the internet and mobile phones (2007) • Directive relating to direct electronic marketing of goods or services (2011) • Directive on video surveillance in public spaces by local authorities (2016) • Directives to banking institutions relating to data retention periods (1/2017 and 2/2017) • Directive on political communications via phone (3/2017) • Directive on the access right of public sector employees (4/2017) • Directive on the retention period of health data (2018) The DPC has become increasingly visible, recently launching a new website with a dedicated section on the provisions of the GDPR. The website contains templates for data breach notifications, complaint forms, as well as for the Data Processing Activities Register (required under Article 30).
Denmark	The Danish Data Protection Agency is on an ongoing basis disclosing various guidelines on the Danish implementation and interpretation of the GDPR, e.g., Guidelines on Security of Processing and Data Protection by Design and by

	Default and Guidelines on the Supervision of Processors and Sub-processors. The latest practice from the Danish Data Protection Agency entails an increased requirement for the use of security measures by private companies, as they are now obligated to employ encryption when transmitting sensitive data and personal identifications number via the internet. Previously this practice solely applied to public authorities. Further, the Danish Data Protection Agency has announced its supervisory control plan for 2018. In 2018, the supervisory entity will focus on selected topics among public and private data controllers. Among private data controllers, the focus will be on supervision of topics such as lawfulness of processing, data security and designation of a DPO.
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).[8] Materials published so far include the following topics: 1) when the appointment of a DPO is required; 2) tasks, knowledge and skills required for DPOs; 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 companies' DPOs 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).[9]
France	The debate was partially focused on the lack of clarity and foreseeability of the FDPA 2 because the recently adopted law will be completed by further implementing decrees to implement the GDPR. In addition, the FDPA may still be subject to major changes in the near future. Indeed, Article 32 FDPA 2 empowers the government to proceed by ordinance to a general rewriting of the FDPA to improve the intelligibility and consistency with all legislation relating to the protection of personal data. This means that the FDPA will undergo major changes in the near future but without any debate before parliament. The government will be able to review the legislation by order within six months as of the enactment of the FDPA 2. During parliamentary procedure, the fact that public entities, such as local authorities, may be fined up to EUR 20 million was highly criticized and some MPs

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

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

	tried to exclude said authorities from being liable under the GDPR. The French Data Protection Authority ("**DPA**") has also planned to establish guidelines, recommendations and benchmarks to facilitate data processing compliance. For instance, the French DPA will provide a list of processing operations subject to mandatory impact assessment and a list of processing operations for which no analysis is required and also a guide to the implementation of the GDPR for small- and medium-sized enterprises.
Germany	The German data protection authorities have issued a wide range of guidance on the GDPR, such as (non-exhaustive list): • consent in accordance with the GDPR • processing of personal data for advertisements • processing in the context of employment • joint controllers • record of processing activities • DPO for controllers and processors • sanctions • data transfer to third countries • DPIA • access rights • transparency requirements • right to be forgotten • special categories of data • risks for the rights and freedoms of natural persons • blacklist for processing activities requiring a DPIA: https://www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf https://www.datenschutzkonferenz-online.de/kurzpapiere.html State data protection authorities have issued additional guidelines and templates for Records of Processing and Data Processing Agreements. Some state data protection authorities have launched online reporting tools for security breaches and to notify the appointment of a DPO. Several German state data protection authorities have launched new websites on which they actively share new statements, FAQs and other helpful information.
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 (i) the application of the GDPR to small- and medium-sized enterprises ("**SMEs**") and whether the penalty exemption applicable to SMEs may be maintained; and (ii) learning courses providing for DPO qualification. (i) Following the publication of the draft GDPR Implementation Act in August 2017, there was public debate about whether Hungary could maintain the penalty exemption applicable to SMEs, which in the past may have received only a warning (rather than a fine) for their first non-compliance with data protection laws. The law designating the Hungarian DPA as a supervisory authority (Act XIII of 2018) says that the DPA should primarily warn SMEs before applying any

	monetary sanctions for non-conformance. However, ultimately, the new law did not maintain the penalty exemption applicable to SMEs. (ii) Because several education service providers advertised their DPO courses misleadingly as "state-approved" courses, the Hungarian DPA released a press statement in April 2018 saying that the DPA does not and will not endorse such courses and that it will not accept the papers issued by such service provider as proof of the DPO's expert knowledge. The Hungarian DPA released a wide range of guidance on the GDPR, including regarding data protection impact assessments (DPIAs), DPOs, the obligation to adopt data protection policies and the application of the GDPR to SMEs. The Hungarian DPA confirmed in April 2018 its guidance that the general impact assessment in the Hungarian legislative process does not exempt a data controller from the obligation to conduct a DPIA related to statutory data processing activities (Article 6(1)(c) and (e) GDPR)[10] because DPIAs were not part of a general impact assessment in the Hungarian legislative process prior to 25 May 2018. Accordingly, the Hungarian DPA expects data controllers to conduct DPIAs even regarding data processing activities based on statutory legal provisions, despite the fact that Hungarian legislation does not expressly iterate the requirement for a DPIA.
Ireland	Some of the most intensely debated subjects in Ireland included: 1. The digital age of consent – throughout the legislative process the government had advocated 13 years of age, but in the end, the opposition parties defeated the government on this issue and the 2018 Act sets the digital age of consent at 16 years. 2. Micro-targeting and profiling of children – Section 30 2018 Act purports to make it an offense for any company or corporate body to process the personal data of a child under 18 years of age for the purposes of direct marketing or profiling. The Office of the Attorney General has advised the government that such a prohibition appears to go beyond the margin of discretion afforded to Member States in giving further effect to the GDPR, and would conflict with Article 6(1)(f), read in conjunction with Recital 47. The government intends to clarify the matter with the European Commission, as the commencement of Section 30 could give rise to a substantial risk of infringement proceedings against Ireland, pursuant to Article 258 of the Treaty on the Functioning of the European Union. 3. The applicability of fines to public bodies – it was originally proposed that a public authority or authority that is not in competition with the private sector would be exempt from administrative fines, but the 2018 Act permits fines of up to EUR 1 million to be imposed on such bodies. 4. Representation of data subjects – the 2018 Act permits a mandated not-for-profit body to bring a representative action on behalf of a data subject seeking injunctive relief or compensation for material or non-material damage suffered as a result of an infringement of data protection law. It remains to be seen whether this means that non-for-profit bodies will be able to take call actions on behalf of multiple data subjects for data breaches, as class actions are not currently permitted under Irish law.
Italy	The most debated points concern: • the appointment of the DPO and, in particular, the technical background (i.e., legal or IT) required to cover this role and the level of the DPO's independence

[10] Under Article 35(10) GDPR the obligation to conduct a DPIA is limited if the controller can rely on legal bases of EU or national law, the law regulates the specific processing operations and a DPIA has already been carried out as part of the legislative procedure. A general impact assessment was already part of the Hungarian legislative procedure, but that assessment did not cover data protection issues.

	• the notification of a data breach and the formalities required to comply with this obligation • 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 • how 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 coexist with the GDPR
Latvia	Given that the fines for violations of personal data processing and enforcement levels in Latvia are currently relatively low, data controllers and processors are mostly concerned with the large amounts of potential 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 with all its tasks and supervising powers provided by the GDPR. There are several proposals by trade/labor unions, hospitals/university hospitals and 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 a person can currently 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	Throughout this tense GDPR-related period, Lithuania came across some emerging and interesting issues: 1. The appointment of the DPO. In particular, the questions arose regarding the technical background (i.e., legal or IT) required to cover this role and the level of the DPO's independence; 2. Criminal background check. It is commonly required by employers or companies that ask for proof that a person (candidate or employee of a service supplier) has not previously been convicted. However, in Lithuania the criminal background check is allowed only in cases provided for in laws, for example, for safe guard positions, civil servants, attorneys, etc. Issues arise when a parent company that is established outside the territory of Lithuania approves policies for affiliates, creating an obligation to check the criminal background of all candidates (or current employees) when there are no legal grounds to do so in Lithuanian law. 3. Sanctions. According to Lithuanian laws, an administrative fine can be imposed on the director or other person who is responsible for personal data breaches in the field of electronic communications. Thus, there might be cases when a personal data breach under the GDPR coincides with an electronic communication data breach. If this is the case, then not only the

	fine foreseen in the GDPR will be imposed on the company, but also an administrative fine under national law imposed on the director of the company and (or) responsible person. This raises certain questions, such as whether such law is in compliance with the general principles for imposing sanctions under the GDPR, as responsibility is only foreseen for legal entities. 4. Data minimization principle. Lithuanian public institutions request private companies to provide documentation to prove their tax relief right. For example, to exercise the right to be exempted from VAT, companies have to submit documentation related to the personal data of their contractors for the Lithuanian State Tax Inspectorate under their request (including photocopies of their IDs, etc.). In most cases, there is no legal ground to require such data under the GDPR and contractors frequently refuse to provide such data. Therefore, businesses are forced to collect personal data which may be in breach of the principle of data minimization to exercise the VAT exemption. In addition, the State Data Protection Inspectorate 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 be in compliance with the new legal regulation on personal data protection in practice. For example, the Inspectorate has prepared: • twelve steps that should be taken to prepare for the GDPR • public consultation on DPOs • information for public authorities and agencies on how to apply the GDPR • recommendations on identification, investigation, reporting and documentation of personal data security breaches • recommendations on records of data processing activities Recommendations on legislative processes regarding national data protection laws supplementing the GDPR.
Luxembourg	There have not yet been any detailed or official indications or topics. The CNPD often publishes guidelines on its website on specific topics, the latest to date was on video surveillance.
Malta	The most intensely debated issues are: 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). 1. 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. 2. 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. 3. 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). 4. 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 safe harbor standard contractual clauses, standard contractual clauses such as the EU Privacy Shield are also still debatable. 5. Privacy Impact Assessments: these will now be mandatory pursuant to Article 35 Regulation 2016/679.
Netherlands	There have not yet been any detailed or official indications or topics.
Poland	The Polish Data Protection Authority has issued limited guidance, in particular regarding (non-exhaustive list): • record of processing activities (with record template) • understanding of the "risk-based approach" • 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 (blacklist). 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 as "trans-border data flows outside the EU."
Portugal	The most intensely debated issues are as follows: • changes to the structure and organization of the CNPD. • sanctions and their application to public entities. • limitations to processing of HR data. • DPO role and requirements. • the right to erasure (right to be forgotten). • child's 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.[11] 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 EU 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 EU 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

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

	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, 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. Exempting 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 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 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 the 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	The authority has recently published two decisions approving (i) the standard application of the data breach notification; and (ii) the receipt and settlement procedure of the complaints. The authority is quite active regarding the GDPR and has 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 the GDPR (e.g., novelty elements brought by the GDPR and 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 GDPR 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 • Practical guide and several legal reports on video surveillance 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 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. The Swedish data protection authority has targeted its first inspection on the compliance of appointing DPOs by private companies and public authorities. The data protection authority has also issued a regulation regarding the processing of

	personal data concerning criminal offenses. In addition, a new camera surveillance act, drafted in light of the GDPR, entered into force 1 August 2018.
UK	The major topics currently debated which have an impact on the application of the GDPR in the UK are related to the consequences of 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. One of the issues 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 proposed (in August 2017) 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). In May 2018 the government advocated a legally binding data protection agreement between the UK and the EU which, according to the government, would bring about more benefits than mutual adequacy recognition.[12] 2. The role of the ICO on the European Data Protection Board ("**EDPB**") and the permanence of the ICO in the EU one-stop-shop mechanism. In May 2018 the UK government proposed[13] as part of its proposal of an EU-UK legally binding data protection agreement (see point 1 above) that the ICO maintain an 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 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. This is currently a debated issue between the EU and the UK and it is one of the aspects which may threaten smooth negotiations over data transfers between the EU and the UK. There is uncertainty on the weight that UK courts will give to the CJEU's jurisprudence following Brexit. It will most likely have persuasive authority. However, the recently adopted European Union (Withdrawal) Agreement 2018 establishes that UK courts will no longer be bound by CJEU's case law laid down on or after Brexit day, and the UK Supreme Court will not be bound by any retained EU case law (i.e., any case law laid down before Brexit day). 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."[14] In July 2018 the House of Commons Committee on Exiting the European Union stated that "the UK should accept, to increase the prospects of securing the Prime Minister's objectives of continuing membership by the Information Commissioner on the European Data Protection Board and representation under the European one-stop shop, that the CJEU will continue to have jurisdiction over aspects of data protection law in the UK after exiting the EU".[15] 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. The ICO has been updating its Guide to the GDPR. This is a living document

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

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

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

[15] House of Commons, Exiting the European Union Committee, "The progress of the UK's negotiations on EU withdrawal: Data," July 2018.

	which the ICO expands over time with the addition of new guidance on various GDPR topics. Recent updates or additions to this guidance concern international data transfers, accountability (including documentation and record of processing), data portability and data protection impact assessments. The ICO has also issued detailed 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 is updating its data sharing code of practice (which is currently subject to public consultation). The ICO has also made a call for evidence on an Age Appropriate Design Code (which is required under the DPA). 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. Finally, following a recent consultation, the ICO's Regulatory Action Policy (required by the DPA) has now been laid down in parliament. It sets out how the ICO plans to discharge its new regulatory powers under the various laws it enforces, including the DPA.

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.