Baker McKenzie.

GDPR National Legislation Survey, 5.0

January 2019

GDPR — National Legislation Survey 5.0 (Update January 2019)

Introduction

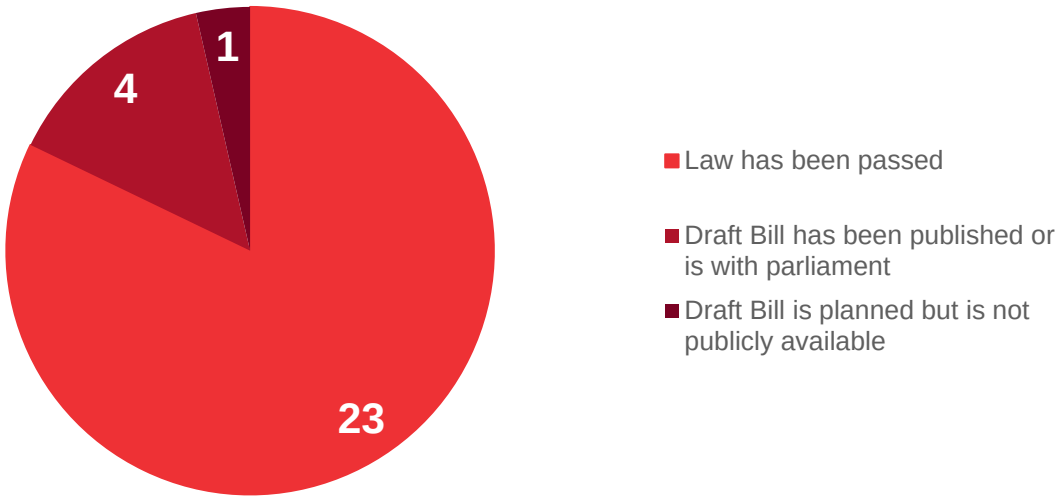
Since 25 May 2018, the EU General Data Protection Regulation (GDPR) applies directly in all EU Member States. The GDPR contains 50+ so-called opening clauses allowing EU Member States to put national data protection laws in place to supplement the GDPR. This survey provides an overview of the current legislative activities in terms of national data protection laws supplementing the GDPR in the 28 EU Member States. We are pleased to make available the 5th edition of this continuously updated survey.

Update January 2019 — Version 5.0

Summary of Findings

I. Countries with National Data Protection Law

Overview of the 28 countries in scope:



- Twenty three countries have passed National Data Protection Laws supplementing the GDPR: **Austria, Belgium, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Romania, Slovakia, Spain, Sweden** and the **United Kingdom**.
- Four countries have published a bill, including a bill that is sitting with parliament: **Bulgaria, Czech Republic, Greece** and **Portugal**.
- In **Slovenia** the new Data Protection Act has not yet been adopted and also its new draft has not yet been published.

II. Age for Minor Consent

According to Art. 8 GDPR, the processing of personal data of a child in relation to the offer of information society services based on the child's consent shall be lawful where the child is at least 16 years of age.

Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorized by the parents or legal guardian. However, Member States may determine a lower age for the child (between 13 and 16 years) where the child consent is sufficient without additional consent or authorization of the parents/legal guardians.

The following age limits for child consents have been provided by the Member States:

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
Cyprus	14	Adopted National Data Protection Law
Czech Republic	(15)*	Draft Bill
Denmark	13	Adopted National Data Protection Law
Estonia	13	Adopted National Data Protection Law
Finland	13	Adopted National Data Protection Law
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	Adopted National Data Protection Act
Latvia	13	Adopted National Data Protection Law
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

Member State	Age Limit	Adopted or Draft Bill
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	Unclear	New Draft Bill not yet published
Spain	14	Adopted National Data Protection Law
Sweden	13	Adopted National Data Protection Law
United Kingdom	13	Adopted National Data Protection Law

* Unofficial statements or draft bills

III. National rules for the processing of data relating to criminal convictions and offenses

According to Article 10, processing of personal data relating to criminal convictions and offenses or related security measures based on Article 6(1) shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

- **Austria:** Data relating to criminal convictions and offenses may be processed if the controller has a prevailing legitimate interest (§ 4 (3)(2) Data Protection Act).
- **Belgium:** Data relating to criminal convictions and offenses may only be processed in specific cases, such as:
  a. by natural or legal persons as necessary for the management of their own litigation
  b. as necessary for archiving purposes, scientific or historical research purposes or statistical purposes
  c. if the data subject explicitly authorized in writing the processing of his/her personal data for one or several purposes, provided that the processing is limited to such purposes
  d. if the processing concerns data manifestly made public by the data subject, on its own initiative, for one or several specific purposes, provided that the processing is limited to such purposes
- **Cyprus:** Data relating to criminal convictions and offenses may be processed for journalistic or academic purposes or for purposes of artistic or literary expression, provided that those purposes are proportionate to the aim pursued and such processing is compliant with the rights set out in the Charter of Fundamental Rights of the European Union and in the European Convention for the Protection of Human Rights and Fundamental Freedoms.
- **Denmark:** 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.
- **Estonia:** The data related to criminal convictions and offenses of a person shall be accessible to another person only if there is a legal basis for accessing such data.

- **Finland:** An organization may process criminal and sanctions data where the processing of such data:
  a. is necessary for the purpose of solving, drafting, presenting, defending or resolving a legal claim
  b. is carried out by an insurance company and the processing is necessary for the determination of the liability of the insurance company
  c. is based on a legal obligation under Finnish law or is necessary for compliance with a legal obligation of the controller
  d. is necessary for scientific or historical research or for statistical purposes
- **France:** Data relating to criminal convictions and offenses may only be processed by a restricted list of controllers. The list includes:
  a. courts, public authorities and legal entities managing public services as part of their statutory missions
  b. court officers acting as part of their statutory missions
  c. certain legal entities mentioned in articles L. 321-1 and L. 331-1 of the French Intellectual Property Code
  d. legal entities and natural persons only for the limited purpose of initiating a lawsuit or enforce a decision
  e. associations appointed by the French "Ministère de Justice" to provide assistance to victims
  f. associations providing assistance to individuals in custody
- **Germany:** Employees' personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason. It is unclear whether Art. 10 GDPR applies also in case of suspected criminal activity. Given recent statements relating to whistleblowing, it seems like the authorities do not consider Art. 10 GDPR applicable for the data processing relating to whistleblowing, i.e., to the processing of suspected criminal offenses.
- **Greece:** Processing of data relating to criminal convictions and offenses is permissible when provided by law which sets the purpose, safeguards and measures for the protection of the data subject rights. As a matter of exception, such processing is also permissible (inter alia) in the context of employment if absolutely necessary for evaluation of suitability for a specific position (relevant information can be obtained by the employee directly from the employer or from a third party on the basis of the employee's prior written consent).
- **Hungary:** Processing of data relating to criminal convictions and offenses is permissible — unless the law provides otherwise — on the legal basis applicable to special categories of personal data (pursuant to Section 5(7) of the Hungarian Information Act), i.e., in practice if the data subject has given explicit consent or if the data processing is necessary for the establishment, exercise or defense of a legal claim.
- **Ireland:** Data relating to criminal convictions and offenses may only be processed in specific circumstances, including with the explicit consent of the data subject, or where the processing is necessary and proportionate for the performance of a contract to which the data subject is a party. Further circumstances may justify the processing under the control of official authority.

- **Italy:** Data relating to criminal convictions and offenses may only be permissible if permitted by law, regulation or, in the absence of the same, by a decree of the Ministry of Justice issued with prior consultation with the Italian data protection authority.
- **Latvia:** Processing of data relating to criminal convictions and offenses is prohibited in the Latvian Employment law (e.g., for background checks), except where the processing is required under respective laws or regulations regulating specific professions (such as teachers and civil servants).
- **Lithuania:** It is prohibited to process personal data related to convictions and criminal offenses of an employee or a candidate who is applying for a job. As an exception, such processing can be lawful if it is required by law to verify the suitability of a certain candidate for the position they applied to.
- **Luxembourg:** Luxembourg has very specific provisions relating to the processing of personal data about convictions and criminal offenses by law enforcement authorities, however, there are no specific provisions for private companies supplementing Art. 10 GDPR.
- **Netherlands:** Personal data of a criminal nature may be processed under a number of general exceptions, for example if it is:
    a. carried out with the data subject's explicit consent for the processing of personal data for one or more specified purposes
    b. necessary to protect the vital interests of the data subject or of another natural person if the data subject is physically or legally incapable of giving consent
    c. related to personal data which are manifestly made public by the data subject
    d. necessary for the establishment, exercise or defense of legal claims or when courts are acting in their judicial capacity
    e. necessary for reasons of substantial public interest as referred to in article 23 (a) and (b) GDPR
    f. necessary for scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) of the GDPR
    g. carried out by bodies that are responsible for applying criminal law pursuant to the Police Data Act or the Judicial Data and Criminal Records Act
    h. carried out by and on behalf of alliances of controllers or groups of controllers governed by public law
    i. necessary for a proper treatment or care of the person concerned
    j. necessary to assess a request from the data subject to take a decision providing services to him or her
    k. necessary to protect the controller's interests in cases of criminal offenses committed against him or which, on the basis of facts and circumstances, can be expected to be committed against him or persons employed by him
    l. carried out for the benefit of a third party by a controller acting pursuant to a license under the Private Security Organizations and Detective Agencies Act or having a license granted by the Dutch DPA
- **Poland:** Only certain sectoral laws have provisions relating to data on criminal convictions and offenses. In particular, employers in certain sectors (e.g., banks, insurers or entities providing certain services to financial institutions) are allowed to conduct limited employee criminal background checks for certain types of employees.

- **Slovakia:** Data relating to criminal convictions and offenses may only be processed on the basis of a specific regulation or international treaty by which the Slovak Republic is bound. By way of example for employment relationships, an employer may request from a natural person information on a clean criminal record only for work where such a clean criminal record is required under the special regulation, or if a clean criminal record is demanded by the nature of work which the natural person is to perform.
- **Spain:** Processing of personal data relating to criminal convictions and offenses by private bodies must be allowed by law, either by a national law or by European Union law. The Spanish DPA specifically allows the processing of this type of data by lawyers and solicitors in the performance of their duties.
- **Sweden:** Processing of personal data concerning criminal offenses by private companies is only permitted if the data concerns individuals holding key or leading positions within the company or the company group if there are objective grounds for processing them in a specific reporting channel (i.e., whistleblowing/ethics hotline) in order to investigate if the individual has committed serious improprieties concerning accounting, internal accounting controls, auditing matters, the prevention of crime (bribery, banking, finance), or other serious improprieties concerning the company's vital interests or the life or the health of an individual.
- **UK:** Data relating to criminal convictions and offenses may only be processed if the processing satisfies predefined conditions under the DPA. This includes, among others, conditions relating to employment, health, substantial public interest and consent.

IV. National rules on the restriction of data subject rights

Union or Member State law to which the data controller or processor is subject may restrict, by way of a legislative measure, the scope of the obligations and rights relating to the data subject rights in Articles 13 through 22 GDPR, and Art. 23 GDPR.

- **Austria:** A controller may deny a data access request if the data contains trade secrets. Also, the provisions on data subject rights do not apply to personal data processing by media undertakings, media services and their employees. If the rectification or erasure is not possible for economic or technical reasons, it is sufficient to restrict the processing as stipulated in Article 18(2) GDPR.
- **Belgium:** Data subject rights are restricted in case of processing of data originating directly or indirectly from certain public authorities. Exceptions to the right to be informed, right of access and right of data portability also apply in relation to controllers who transfer personal data to the such authorities.
- **Croatia:** The Croatian DPA does not make use of Article 23 GDPR restrictions directly, but it does make use of the opening clause in Article 89 GDPR allowing for certain restrictions of data subject rights in relation to data processing for statistical purposes.
- **Cyprus:** A controller may be exempt (in whole or in part) from the duty to communicate a personal data breach to the data subject (on any of the grounds set out under Article 23(1) GDPR). In this case, prior consultation of the Commissioner for Personal Data Protection is required.
- **Denmark:** Data subject rights may be limited, if:
    a. 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
    b. 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

- **Estonia:** The rights of the data subjects may be restricted in case of processing of personal data by law enforcement agencies for the purposes of prevention, detection or prosecution of criminal offenses, or the execution of criminal penalties.
- **Finland:** The Finnish DPA provides for several restrictions, such as:
    a. Article 14 of the GDPR is restricted where the provision of information causes material injury or harm to the data subject and the relevant personal data is not used in decision-making regarding the data subject in question.
    b. Article 15 of the GDPR is restricted where access to the personal data: (i) could harm public order and security, or hinder the prevention or investigation of criminal offenses; or (ii) could cause a serious risk to the health or treatment of the data subject, or to the rights of the data subject or of a third party; or (iii) is used for control and inspection purposes and the non-disclosure of such personal data is necessary in order to safeguard an important economic or financial benefit of Finland or the European Union.
    c. Other data subject rights re restricted where personal data is processed for purposes of scientific or historical research, statistical purposes, for journalistic, academic, artistic or literary purposes, or for public interest archiving purposes.
- **France**:
    a. Data subject rights are restricted if state security, intelligence services, public defense or public security are at stake.
    b. Data subject rights are restricted when the processing is carried out by law enforcement agencies.
- **Germany:** The German DPA provides for several restrictions, such as:
    a. In case of processing for scientific or historical research or statistical purposes, data subject rights pursuant to Art. 15, 16, 18 and 21 GDPR shall be limited to the extent that these rights are likely to render impossible or seriously impair the achievement of the scientific or historical research or statistical purposes; the access right pursuant to Art. 15 GDPR shall not apply in case of scientific research if access to the data would involve disproportionate efforts.
    b. In case of processing for archiving purposes in the public interest, Article 15 GDPR shall not apply if the archived data is not identified with the person's name or if the identification of the data would require unreasonable administrative efforts and Article 16 GDPR shall not apply at all, however, the data subject may request that his or her corrections are added to the archived file, and certain rights under Art. 18, 20, and 21 GDPR shall not apply if they likely render impossible or seriously impair the achievement of the archiving purpose.
    c. Art. 13 (3) GDPR relating to information about the intended secondary processing purposes is restricted in certain circumstances, such as interference with the establishment, exercise or defense of legal claims, in which case the controller must provide such information typically to the public.
    d. Art. 13 (3) GDPR is restricted where personal data is transferred to a lawyer in the context of an attorney-client relationship.
    e. Art. 14 (1) to (4) GDPR shall not apply as far as meeting this obligation would disclose information which by its nature must be kept secret, in particular because of overriding legitimate interests of a third party.
    f. Art. 14 (1), (2) and (4) GDPR may not apply for private bodies where meeting this obligation would interfere with the establishment, exercise or defense of legal claims, or processing includes data from contracts under private law and is intended to prevent harm from criminal offenses, or where

disclosing the data would endanger public security, in which case the controller must provide such information typically to the public.

g. Art. 15 GDPR shall not apply: (i) as far as access would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party; (ii) where disclosing the data would endanger public security; (iii) where the data is retained only for purposes of compliance with legal or statutory retention requirements; or (iv) where the data is processed only for purposes of monitoring data protection, and in cases (iii) and (iv), providing the information would require a disproportionate effort and appropriate technical and organizational measures make processing for other purposes impossible.

h. Art. 17 GDPR shall not apply in case of lawful non-automated processing where the deletion is impossible or requires a disproportionate effort due to the specific type of storage and the interests of the data subject are rather low. In this case, further processing must be restricted.

i. Art. 17 para. 1 (a) and (d) GDPR shall not apply as long and as far as the controller has reason to believe that erasure would adversely affect legitimate interests of the data subject.

j. Art. 34 GDPR (obligation to inform a data subject of a personal data breach) shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party, unless the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

- **Greece:** The controller can (partially of fully) refuse a data subject right if processing is related to:

  a. national security

  b. defense

  c. public security

  d. the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security

  e. important economic or financial interest of the Greek state

  f. the establishment, exercise or enforcement of law claims

  g. the protection of the data subject or the rights and freedoms of others

- **Ireland:** Data subject rights may be restricted where necessary and proportionate in specific circumstances, including for the exercise or defense of legal claims or legal proceedings, for the enforcement of civil law claims, and where the information is protected by legal privilege.

  An individual's right under Article 15 to obtain a copy of his/her personal data may be further restricted in certain cases, e.g., where in the opinion of a health practitioner the supply of health data would cause serious harm to his or her physical or mental health.

- **Italy:** Data subject rights may be restricted, in addition to the limitations provided by the GDPR, only in the specific circumstances set forth in the Italian GDPR alignment law, such as in case of defensive investigations, in relation to the enforcement of rights in judicial cases and to protect the confidentiality of an employee who files a report under a whistleblowing scheme set up as provided under the law. When a data subject's rights may be compromised, it is possible to revert to the Garante (the Italian data protection authority) for their enforcement, and companies have an obligation to inform the data subjects of this right.

- **Latvia:** The data access right does not apply, if it is prohibited to disclose such information in accordance with the laws and regulations regarding national security, national protection, public safety and criminal law, as well as for the purpose of ensuring public financial interests in the areas of tax protection, prevention of money laundering and terrorism financing, ensuring the supervision of financial market participants and functioning of guarantee systems thereof, or for the application of regulations and macroeconomic analysis. Furthermore, the law provides a possibility to restrict other data subject rights provided in other laws and regulations in accordance with Article 23 GDPR.

  Additionally, other data subject rights can be restricted where personal data is processed for journalistic, academic, literary purposes, for the interests of freedom of expression as well as for the processing for archiving purposes in the public interest, scientific, historical research purpose or statistical purposes.

- **Netherlands:** The Dutch DPA provides for several restrictions, such as:

  a. Art. 34 GDPR (obligation to inform a data subject of a personal data breach) shall not apply to financial institutions

  b. data subject rights vis-à-vis public registers are restricted

- **Poland:** The Polish DPA provides for several restrictions, such as:

  a. Articles 15, 16 and 18 to 22 GDPR do not apply to certain processing activities of the press as well as to literary or artistic expression.

  b. Art. 15 (3) and (4) GDPR and Art. 18 GDPR shall not apply to the processing of personal data for the purposes of academic expression.

  c. Art. 15 (1) to (3) GDPR may be restricted in case of controllers performing public tasks if such restriction serves the purpose of performing a public task, provided that certain additional conditions have been met.

- **Slovakia:** The data subject rights may be limited in order to safeguard the interests outlined in Article 23 GDPR, with the addition of economic mobilization.

- **Spain:** The PDPA allows that the lawmakers adopt specific provisions to restrict data subject rights described in Articles 12 to 22. However, such specific provisions have not yet been adopted.

- **Sweden:** The Swedish DPA provides for several restrictions, such as:

  a. The right to information and access to the personal data (Art. 13 to 15 GDPR) does not apply to data that is subject to secrecy regulation. This applies also to private organizations as regards information that should have been exempted from the right to information pursuant to the Public Information to Access and Secrecy Act (2009:400) that applies to public authorities.

  b. The right of access (Art. 15 GDPR) does not apply to personal data contained in running texts that constitute rough drafts or notes, unless the personal data has been transferred to a third party, the personal data is processed for archiving or statistic purposes or has been processed longer than one year.

- **UK:** The DPA provides for certain exemptions in relation to data subject rights which apply in the context of, among others, crime, taxation, immigration and journalism.

V. National rules on DPOs

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:

- **Belgium:** An organization must appoint a DPO in certain situations where the processing of personal data is likely to result in a high risk (as referred to in Article 35 GDPR), e.g., (i) when it processes personal data on behalf of the federal police service or the federal police service transfers personal data to it and (ii) in the context of processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.
- **Cyprus:** The data protection authority may publish a list of circumstances under which the appointment of a DPO is required, beyond the requirements set out in Article 37(1) GDPR.
- **Finland:** There is some prior Finnish legislation that sets the requirements for certain organizations operating in the field of healthcare or social welfare, such as drugstores and healthcare service providers, to appoint a DPO. In addition, the Finnish DPA defines certain special situations in which the entity must assess whether the appointment a DPO is necessary. Appointment of a DPO is one of the safeguarding measures available to the entity, not a mandatory requirement in each of the situations defined in the Finnish DPA.
- **Germany:** In addition to Art. 37(1) GDPR, controllers and processors must designate a DPO, if they permanently employ at least ten employees dealing with the automated processing of personal data, or if they are required to carry out a privacy impact assessment pursuant to Article 35 GDPR, or if they commercially process personal data for the purpose of transfer, anonymized transfer, or for purposes of market or opinion research.
- **Romania:** Controllers and processors must appoint a DPO in case of processing of a national identification number for a controller's legitimate interest.
- **Spain:** Certain entities are required to appoint a DPO pursuant to the Spanish DPA. 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.

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

- **Greece:** Controllers and processors must appoint a DPO if the processing operations, according to the authority's relevant issued catalogue, require regular and systematic monitoring of data subjects on a large scale by virtue of their nature, their scope and/or their purposes.

VI. National rules providing for restrictions on the transfer of sensitive data to third countries without an adequacy decision

In the absence of an adequacy decision, Union or Member State law may, for important reasons of public interest, expressly set limits on the transfer of specific categories of personal data to a third country or an international organization. According to Article 49 (5), Member States shall notify such provisions to the Commission.

The following Member State provides national rules for restrictions on the transfer of sensitive data to third countries without an adequacy decision.

- **Cyprus:** The supervisory authority may, on grounds of public policy, impose restrictions on the transfer of special categories of data to a third country or an international organization. To that end, a controller or processor must notify the authority of its intention to transfer special categories of data to a third country or an international organization.

VII. National rules for the processing of national IDs

According to Article 87, Member States may further determine the specific conditions for the processing of a national identification number or any other identifier of general application. In that case, the national identification number or any other identifier of general application shall be used only under appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation.

The following Member States have defined national rules for the processing of national IDs:

- **Belgium:** As a general rule, a specific authorization of principle is required for the use of the identification numbers of the National Registry.
- **Denmark:** Private companies may process personal identification numbers, where:
  a. this follows from the law
  b. the data subject has given consent (in compliance with the conditions laid down in Article 7 GDPR)
  c. the processing is carried out solely for scientific or statistical purposes
- **Finland:** The Finnish DPA provides that a personal identification number may be processed on the unambiguous consent of the data subject or where so provided by law. A personal identification number may also be processed if it is necessary to unambiguously identify the data subject: (i) in order to perform a task laid down by law; (ii) in order to realize the rights or duties of the data subject or the controller; or (iii) for the purposes of historical, scientific or statistical research. A personal identification number may also be processed in activities relating to the granting of credit and the collection of debt, in the insurance, credit, payment, renting and lending businesses, in credit data operations, in healthcare, in social welfare activities or other social services and in matters relating to the civil service, employment and other service relationships and benefits to the same. Further, a personal identification number may be disclosed for the purposes of updating of address information and prevention of redundant postal traffic, provided that the personal identification number is already available to the recipient. The controller shall ensure that the personal identity number is not unnecessarily included in hard copies printed or drawn up from the filling system.
- **France:** Processing of national IDs (i.e., data including registration number in the French national identification register, the "NIR") is subject to specific requirements determined by a decree of the French Conseil d'Etat. This decree (still to come) will enumerate the categories of controllers and the purposes for which the processing of the national ID will be permitted. However, the processing restriction will not apply to the following purposes:
  a. statistical purposes implemented by the national statistical service (provided no sensitive data or data relating to criminal offenses is processed);
  b. exclusively scientific or historical purposes; or for supplying users with one or more online government services, under certain conditions;
  c. purposes to make available one or more electronic administration services to users of the administration, those services are defined in Article 1 of Order No. 2005-1516 of 8 December 2005 on electronic exchanges between users and administrative authorities and between administrative authorities themselves.

  For exceptions relating to statistical purposes and scientific research purposes, the NIR processing must first be subject to a cryptographic operation replacing it with a non-significant statistical code.
- **Hungary:** The tax ID, national identification number and social security ID may be processed only if there is a legal obligation to process this data or if the data subject has given written (i.e., wet signature) consent to the data processing.

- **Lithuania:** It is prohibited to process a person's national ID for direct marketing purposes. It is also not permitted to make a person's national ID public.
- **Netherlands:** The citizen service number (in Dutch: "burgerservicenummer"), which is displayed on national ID documents, may only be processed on the basis of a specific statutory obligation. Otherwise the processing is prohibited.
- **Romania:** The processing of a national ID number, including the collection or disclosure of documentation which contains the national ID number processed based on Art. 6, par. (1), lit. (f) GDPR, shall be carried out by the data controller only if it has implemented specific safeguards, such as implementing appropriate technical and organizational measures and appointing a data protection officer.
- **Slovakia:** Processing of personal identification numbers for the purpose of identifying a data subject is permissible only if such processing is necessary to achieve the intended purpose of the processing.
- **Spain:** Regarding the processing of national IDs, the Personal Data Protection Act sets forth specific rules only for those cases in which the data controller is a public body.
- **Sweden:** Absent a 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.

VIII. National rules for filings and/or notifications with the national data protection authority

- **Belgium:** As a general rule, a controller must notify processing activities in relation to the installation of CCTV cameras and obtain an authorization of principle for the communication of health data.
- **Cyprus:** Prior notification to the Data Protection Commissioner (the DPC) is required where special categories of data are to be transferred to third countries. Prior consultation with the DPC is required:

  a. 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

  b. 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

  Also, a controller must notify the DPC in writing of the use of CCTV, including an explanation of the purpose and reason for its use.
- **Denmark:** Pursuant to the Danish Data Protection Act, a company needs to notify the Danish Data Protection Agency for example when the company is processing sensitive data (cf. GDPR Article 9 (1) based on substantial public interests, cf. the Danish Data Protection Act section 7 (4)).
- **Finland**: No general rules for filings or notifications apply. However, for the protection of personal data processed in connection with scientific and historical research or statistical purposes, the Finnish DPA requires that a data protection impact assessment is conducted. Thereinafter, a written notification, including the conducted DPIA, shall be submitted to the Finnish supervisory authority, i.e., the Data Protection Ombudsman, before the processing is commenced.

  The above-mentioned requirements apply only in cases where the controller intends to deviate from the data subject rights laid down in the GDPR, and in such cases, the processing is also subject to the following preconditions:

  a. the processing is based on an appropriate research plan

  b. there is a responsible person or group of the research

c. personal data is processed or disclosed only for the purposes of historical or scientific research, or other similar purposes and the operations are conducted in such a manner that third parties do not become aware of the personal information regarding a specific person

- **France:** Prior notification and authorization is required

  a. for health data

  b. in the public sector

  c. for data processing carried out by data controllers in the following French overseas territories until the Executive Order of 12 December 2018 comes into force: New Caledonia, Wallis and Futuna, French Polynesia, French Southern and Antarctic Lands

- **Hungary:** The controller has an obligation to notify Hungary's Chief Public Health Officer of the international transfer of genetic data and genetic samples for the purpose of human genetic research and human genetic testing. That notification must contain a reference to the appropriate adequacy safeguards provided by the exporter/importer.

- **Italy:** The controller must notify the data processing based on legitimate interest in some limited cases, notably when the processing is functional to the authorization of the change of name or surname of minors, thus limiting the procedure to performance of public interest tasks that may present a high risk.

- **Spain:** The Spanish DPA sets forth notification and consultation obligations with the Spanish authority regarding opt-out lists from commercial communications ("Robinson lists").

- **UK:** The UK data protection authority requires payment of a "Data Protection Fee" by organizations and sole traders, unless they are exempt. There are three levels of fee corresponding to the organizations size. The grounds for exemption are quite complex and limited, and generally only apply if the entity is processing data relating to its own internal business operations.

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 Contacts 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 Caroline Sieveritz 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

Magalie Dansac Le Clerc
Partner, Paris
+ 33 1 44 17 59 82
magalie.dansacleclerc
@bakermckenzie.com

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 89 552 38 242
julia.kaufmann@bakermckenzie.com

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

Michaela Nebel
Partner, Frankfurt
+49 69 299 08368
michaela.nebel@bakermckenzie.de

Yann Padova
Partner, Paris
+ 33 1 44 17 59 23
yann.padova@bakermckenzie.com

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

Michael Schmidl
Partner, Munich
+49 89 552 38 155
michael.schmidl@bakermckenzie.com

Matthias Scholz
Partner, Frankfurt
+49 69 299 08180
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, Erik Steiner (Baker McKenzie)
Belgium	Elisabeth Dehareng (Baker McKenzie)
Bulgaria	Violetta 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, Benedikt Vogel (Baker McKenzie)
Greece	George Ballas, Theodore Konstantakopoulos (Ballas, Pelecanos & Associates)
Hungary	Ines Radmilovic, Adam Liber (Baker McKenzie)
Ireland	Davinia Brennan (A&L Goodbody)
Italy	Francesca Gaudino (Baker McKenzie)
Latvia	Sarmis Spilbergs, Edvijs Zandars, Liga Merwin, Mikijs Zimecs (Ellex Klavins)
Lithuania	Jaunius Gumbis, Migle Petkevičienė, Rolandas Valiunas, Tomas Kamblevicius, Kristupas Spirgys (Ellex Valiunas)
Luxembourg	Sybille Briand, Laurent Fessmann (Baker McKenzie)
Netherlands	Nathalja Doing, Wouter Seinen, Andre Walter (Baker McKenzie)
Poland	Magdalena Kogut-Czarkowska, Radoslaw Nozykowski (Baker McKenzie)
Portugal	Ricardo Henriques (Abreu Advogados)
Romania	Bogdan Mihai, Iulian Popescu (Musat & Asociatii)
Slovakia	Milena Hoffmanova (Baker McKenzie)
Slovenia	Markus Bruckmüller, Klara Miletic (Wolf Theiss)
Spain	Raul Rubio, Ignacio Vela (Baker McKenzie)
Sweden	Jennie Nilsson, Margarita Kozlov (Baker McKenzie)
United Kingdom	Benjamin Slinn, Maura Migliore (Baker McKenzie)

Question 1 — Adopted National Data Protection Laws

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. a link to such National Data Protection Law (local language and/or English as available)

b. a high-level overview of the key provisions of the National Data Protection Law

c. details on how the National Data Protection Law made use of specific opener clauses of the GDPR, in particular:

   i. Article 8 GDPR (age for minor consent)

   ii. Article 10 GDPR (processing of data relating to criminal convictions and offenses especially in the employment relationship, e.g., background checks, whistleblowing hotlines, internal investigations)

   iii. Article 23 GDPR (relevant restrictions on data subject rights)

   iv. Article 37(4) GDPR (additional thresholds requiring the appointment of a DPO)

   v. Article 49(5) GDPR (restrictions on the transfer of sensitive data to third countries without an adequacy decision)

   vi. Article 87 GDPR (specific rules for the processing of national IDs)

   vii. any requirements for filings and/or notifications with the national data protection authority

Austria

Links to the National Data Protection Law

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 — available here:

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

Furthermore, the Austrian data protection authority issued a list of processing operations (Article 35(4) GDPR — "blacklist") which require a data protection impact assessment in November 2018:

https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010375

High-level overview of the key provisions of the National Data Protection Law

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, in general, to implement only 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). Details on how the National Data Protection Law made use of specific opener clauses of the GDPR The controller can deny a request of access by the data subject if the information contains trade secrets. Media undertakings, media services and their employees are exempt from the applicability of 1. Chapter II (principles), with the exception of Article 5 2. Chapter III (rights of the data subject) 3. Chapter IV (controller and processor), with the exception of Articles 28, 29 and 32 4. Chapter V (transfer of personal data to third countries or international organizations) 5. Chapter VI (independent supervisory authorities) 6. Chapter VII (cooperation and consistency) 7. Chapter IX (specific data processing situations) of the GDPR in regard to the processing of personal data for journalistic purposes There are no formal requirements for filings or notifications with the Austrian data protection authority.
Belgium	Links to the National Data Protection Law The Belgian Parliament has adopted four acts to supplement the GDPR: 1. The Act of 3 December 2017 on the creation of the Belgian Data Protection Authority — "*Loi portant création de l'Autorité de protection des données*" available in French at: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2017120311&table_name=loi and "*Wet tot oprichting van de Gegevensbeschermingsautoriteit*" available in Dutch at: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2017120311&table_name=wet 2. The Act of 21 March 2018 amending the existing Belgian Act of 21 March 2007 on camera surveillance — "*Loi modifiant la loi sur la fonction de police, en vue de régler l'utilisation de caméras par les services de police, et modifiant la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, la loi du 30 novembre 1998 organique des services de renseignement et de sécurité et la loi du 2 octobre 2017 réglementant la sécurité privée et particulière*" available in French at: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2018032121&table_name=loi and "*Wet tot wijziging van de wet op het politieambt om het gebruik van camera's door de politiediensten te regelen, en tot wijziging van de wet van 21 maart 2007 tot regeling van de plaatsing en het gebruik van bewakingscamera's, van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten en van de wet van 2 oktober 2017 tot regeling van de private en bijzondere veiligheid*" available in Dutch at: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2018032121&table_name=wet 3. The Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data — "*Loi relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel*" available in French at: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&table_name=loi&cn=2018073046

and "*Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens*" available in Dutch at:

http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2018073046&table_name=wet

4. The Act of 5 September 2018 establishing the information security committee and amending various acts regarding the implementation of Regulation (EU) 2016/679 — "*Loi instituant le comité de sécurité de l'information et modifiant diverses lois concernant la mise en oeuvre du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE"* in French available at:

   http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2018090501&table_name=loi

   and "*Wet tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679"* in Dutch available at:

   http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2018090501&table_name=wet

High-level overview of the key provisions of the National Data Protection Law

Firstly, the Act of 3 December 2017 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. It creates and regulates the functioning of the new Belgian Data Protection Authority that has replaced the former Belgian Privacy Commission. The new Belgian 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, the Act of 21 March 2018 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 new Belgian Data Protection Authority and establishment of a record of processing activities by the controller).

Thirdly, the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data was adopted on 19 July 2018 and published on 5 September 2018. This act revoked the existing Data Protection Act of 8 December 1992.

Fourthly, the Belgian Act of 5 September 2018 (published on 10 September 2018) established a new information security committee, which took over certain competences of the former sectorial committees that existed within the Privacy Commission.

Some notable provisions covered by the Act of 30 July 2018 include:

1. 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
2. restrictions to data subject rights in specific circumstances
3. special rules for the processing of personal data in the public sector, as well as by specific authorities (e.g., police services)
4. particular provisions with regard to the processing for journalistic purposes and the purposes of academic, artistic or literary expression
5. provisions applying to the processing of personal data for archiving purposes in the public interest, for scientific or historical research purposes or statistical purposes
6. specific remedies and representation of data subjects
7. specific sanctions

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

1. **Article 8 GDPR (age for minor consent)**

   The minimum age required for lawful processing based on consent in relation to the offer of information society services to a child is set at 13 years old. Below the age of 13 years, parental consent is required.

2. **Article 10 GDPR (processing of data relating to criminal convictions and offenses)**

   The Act of 30 July 2018 provides that the processing of personal data relating to criminal convictions and offenses is permitted:

   i. by natural or legal persons as necessary for the management of their own litigation

   ii. by attorneys or other legal counsels as necessary for the defense of their clients

   iii. by other persons as necessary for reasons of substantial public interest for the performance of a task carried out in the public interest assigned by or by virtue of a law, Decree or Ordinance or EU law

   iv. as necessary for archiving purposes, scientific or historical research purposes or statistical purposes

   v. if the data subject explicitly authorized in writing the processing of his/her personal data for one or several purposes, provided that the processing is limited to such purposes

   vi. if the processing concerns data manifestly made public by the data subject, at their own initiative, for one or several specific purposes, provided that the processing is limited to such purposes

   As additional measures for such processing, this Act provides that the controller (and, as the case may arise, the processor) must:

   i. Establish a list of the categories of persons having access to the personal data relating to criminal convictions and offenses or related security measures, including a description of their function in relation to the data. This list must be made available to the competent supervisory authority upon request.

   ii. Ensure that such persons have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

3. **Article 23 GDPR (relevant restrictions on data subject rights)**

   The Act of 30 July 2018 prescribes restrictions to data subject rights and to the principle of transparency in case of processing of data originating directly or indirectly from certain authorities such as National Security and Intelligence Services, the Army, authorities of classification and security clearances, OCAM/OCAD, the Passenger Information Unit (PNR data), etc.

   Besides, exceptions to the right to be informed, right of access and data portability also apply for controllers who communicate personal data to the such authorities.

   Where personal data appears in a judgment or a judicial record or are subject to processing as part of a judicial investigation or a criminal procedure, the data subject rights are exercised in accordance with the Judicial Code, the Code of Criminal Procedure, to the special laws relating to criminal procedure as well as implementation decrees.

4. **Article 37(4) GDPR (additional thresholds requiring the appointment of a DPO)**

   The Act of 30 July 2018 states that a private body which processes personal data on behalf of a federal public authority or to whom a federal public authority transfers personal data must appoint a DPO where the processing of such data is likely to result in a high risk to the rights and freedoms of natural persons (as referred to in Art. 35 of the GDPR with regard to DPIA).

   In the context of processing for archiving purposes in the public interest,

scientific or historical research purposes or statistical purposes, the controller must appoint a DPO where the processing of personal data is likely to result in a high risk as referred to in Article 35 GDPR.

5. Article 87 GDPR (specific rules for the processing of national IDs)

The Act of 30 July 2018 does not contain any specific provision determining specific conditions for the processing of the national identification number, i.e., the National Registry Number.

However, the processing and transfer of the Belgian National Registry Number (corresponding to the Social Security Number) is strictly regulated under the Act of 8 August 1983 organizing a National Registry for natural persons, available in French at:

http://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?language=fr&la=F&cn=1983080836&table_name=loi&&caller=list&F&fromtab=loi&tri=dd+AS+RANK&rech=1&numero=1&sql=%28text+contains+%28%27%27%29%29

and in Dutch at:

http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=1983080836&table_name=wet

Pursuant to this Act of 8 August 1983, a specific authorization of principle is required for the use of the identification numbers of the National Registry (see the Act of 5 September 2018 establishing the committee which is competent for those authorizations).

6. Requirements for filings and/or notifications with the national data protection authority

i. CCTV Notification

Under the Act of 21 March 2007 regarding the installation of surveillance camera, as amended by the Act of 21 March 2018, available in French at:

http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2007032139&table_name=loi

and in Dutch at:

http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2007032139&table_name=wet

the decision to install a surveillance camera and to modify such surveillance system must be notified to the police services on a platform provided by the Public federal Service Interior at www.declarationcamera.be (and no longer to the Belgian Data Protection Authority).

ii. Authorization of principle for the communication of health data

Pursuant to Article 42, § 2, 3 of the Act of 13 December 2006 containing various health provisions, as amended by the Act of 5 September 2018, available in French at:

http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2006121335&table_name=loi

and in Dutch at:

http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2006121335&table_name=wet

any communication of personal data relating to health is subject to an authorization of principle of the Social Security and Health Chamber of the Information Security Committee ("*comité de sécurité de l'information*" or "*Informatieveiligheidscomité*"). The scope of this requirement and the relevant exceptions are not very clear and should, therefore, be checked on a case-by-case basis with this Committee (which has just been created).

Bulgaria	N/A — no adopted National Data Protection Law yet
Croatia	**Link to the National Data Protection Law** 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 is available here: https://narodne-novine.nn.hr/clanci/sluzbeni/2018_05_42_805.html **High-level overview of the key provisions of the National Data Protection Law** 1. 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. 2. 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 by the data subject's explicit consent. This applies to all data subjects who enter into life insurance agreements and agreements with endowment clauses in Croatian territory if the data controller is located in Croatia or is providing services in Croatia. 3. The 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. 4. 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. **Details on how the National Data Protection Law made use of specific opener clauses of the GDPR** **1. Data subject rights** The Act does not make use of Article 23 GDPR restrictions directly, but it does make use of the opening clause in Article 89 GDPR which enables certain restrictions of data subject rights in relation to data processing for statistical purposes. In terms of processing of personal data for purpose of producing official statistics, the bodies producing such statistics are not obliged to provide data subjects with the right of access, right to rectification, right to restriction of processing and right to object to processing of personal data so as to ensure conditions necessary for achieving the purpose of official statistics, in so far as such rights are likely to render impossible or seriously impair the achievement of that purpose and when such derogations are necessary for the fulfillment of that purpose. When transferring personal data for purposes of official statistics, data controllers are not obliged to notify data subjects of the transfer. **2. Specific rules for the processing of national IDs (Art 87 GDPR)** The Act itself does not provide any specific rules for the processing of national IDs, but the (preexisting) Act on Personal Identification Number and Bylaws on Personal Identification Number regulate the manner of issuing and use of personal identification numbers in Croatia.

Cyprus	**Links to the National Data Protection Law** 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 — available: 1. in Greek at: http://www.cylaw.org/nomoi/enop/non-ind/2018_1_125/full.html 2. in English (unofficial version) at: http://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/BAE2F781893BC27DC225820A004B7649/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf?openelement **High-level overview of the key provisions of the National Data Protection Law** 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 allowed under the Law. 2. An express prohibition on the processing of genetic and biometric data for the purposes of life and health insurance is included in the Law. 3. The Law stipulates that a controller can restrict (in whole or part) the rights set out in Articles 12, 18, 19 and 20 GDPR, but must consult with the Commissioner prior to restricting any rights of a data subject. Where such restrictive measures involve a processor, these measures must be implemented subject to the provisions of Article 28 GDPR. The DPC may impose restrictions and terms in this regard. 4. The Law provides that the accreditation of certification bodies in Cyprus will be performed by the Cyprus Organization for the Promotion of Quality. **Details on how the National Data Protection Law made use of specific opener clauses of the GDPR** The key provisions of the Law are summarized below: 1. 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). 2. The prior consultation of the Commissioner for Personal Data Protection, the "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). 3. 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. 4. Regarding third country transfers, the Law provides that: i. 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 ii. 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 iii. 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) iv. 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 5. The Law sets out a number of administrative and criminal offenses. In the case of criminal liability where the processor or controller concerned is: i. an undertaking or a group of undertakings, criminal liability rests with the chief executive body of the undertaking or group of undertakings concerned ii. 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 6. The processing of personal data relating to criminal convictions and offenses is permitted where this is carried out for journalistic or academic purposes (or for purposes of artistic or literary expression), provided that those purposes are proportionate to the aim pursued and such processing is compliant with the rights set out in the Charter of Fundamental Rights of the European Union and in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). 7. In the context of the interconnection of filing systems, where the interconnection is to be carried out with the use of identity card numbers or any other identifier of general application, a data protection impact assessment must be carried out as well as prior consultation with the DPC. The DPC has the power to impose restrictions on such interconnections. 8. The use of CCTV must be notified in writing to the DPC with an explanation of the purpose and reason for its use.
Czech Republic	N/A — no adopted National Data Protection Law yet.
Denmark	High-level overview of the key provisions of the National Data Protection Law The Danish Data Protection Act ("Act") entered into force along with the GDPR. 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: 1. 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 2. 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. Additionally, 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. Details on how the National Data Protection Law made use of specific opener clauses of 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 ii. the processing is necessary for the purpose of safeguarding a legitimate interest that clearly overrides the interests of the data subject 3. 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. 4. The Act limits the data subject 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 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 5. 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 iv. if the other conditions laid down in Article 7 GDPR are satisfied 6. Pursuant to the Danish Data Protection Act, which entered into force along with the GDPR, a company needs to notify the Danish Data Protection Agency when the company: i. is using warning registers, credit rating agencies and judicial information systems (cf. the Danish Data Protection Act section 26 (1)) ii. is processing sensitive data (cf. GDPR Article 9 (1) based on substantial public interests, cf. the Danish Data Protection Act section 7 (4)) iii. intends to disclose statistical or scientific studies to a third party pursuant to the Danish Data Protection Act — section 10 (1) (cf. section 10 (3)) The Danish Minister of Justice may, under the provisions of the Danish Data Protection Act, lay down rules on payment of fees for the submission of the above-mentioned applications/notifications. However, the Minister of Justice has not yet imposed any fees or rules of payment.
Estonia	Link to the National Data Protection Law In August 2018, the government of Estonia introduced the Draft Bill for the new Personal Data Protection Act (the "Act") to the Parliament. The Act entered into force on 15 January 2019. The Act is available on the website of the Estonian Parliament (in Estonian only) at: https://www.riigiteataja.ee/akt/104012019011 High-level overview of the key provisions of the National Data Protection Law The Act replaces the Personal Data Protection Act. The purpose of the Act is to specify and supplement the GDPR and to transpose Directive 2016/680. Some notable provisions of the Act are: 1. Provisions regarding fewer restrictions in case of processing personal data for

	journalistic purposes, for academic and artistic expression, for scientific, historical research or statistical purposes, and for archiving purposes in the public interest. 2. The consent of the data subject, given while he/she was alive, shall be valid in his/her lifetime and for 10 years after the death of the data subject (20 years if the data subject was under 18 at the time of death). After death, the processing of personal data of the data subject is permitted under the consent of an heir. 3. In case of enforcement of civil law claims, personal data can be transferred and processed to assess the creditworthiness of a data subject, unless certain restrictions specified in the Act are applied. 4. In case of video or audio recordings made in public space or public events for the purpose of publication, the consent of the data subject may be either presumed or replaced by notifying the data subject of such processing. 5. The Act establishes that the supervisory authority in the meaning of GDPR Article 51 (1) shall be the Estonian Data Protection Inspectorate and grants to the Inspectorate the competence to carry out state and administrative supervision. Details on how the National Data Protection Law made use of specific opener clauses of the GDPR 1. The age for minor consent is 13. 2. In Estonia, data related to criminal convictions and offenses is stored in the State Criminal Records Database. There is a draft bill in the parliament that shall amend the current Criminal Records Database Act so that data relating to criminal convictions and offenses about a person shall be accessible to another person only in case there is a legal basis for accessing such data. 3. The rights of the data subjects may be restricted in case of processing of personal data by law enforcement agencies for the purposes of prevention, detection or prosecution of criminal offenses or the execution of criminal penalties, in which case the rights of the data subject to be informed of the processing of their personal data, to obtain information from the controller and access their personal data, and to be notified in case of a personal data breach, may be restricted in the cases prescribed by law if exercising these rights may: i. hinder or damage the prevention, detection or prosecution of a criminal offense or the execution of criminal penalties ii. damage the rights and freedoms of others iii. endanger national security iv. endanger the protection of public order v. hinder an official investigation or proceedings 4. There are no additional thresholds regarding the appointment of a DPO. 5. The Act specifies the conditions whereby the transfer of data to third countries without an adequacy decision is permitted, however, there are no specific rules or restrictions regarding the transfer of sensitive data. 6. There are no specific rules for processing national IDs. 7. There are no additional filing or notification obligations.
Finland	Link to the National Data Protection Law On 1 March 2018, the Finnish government gave its proposal regarding the adoption of a new Data Protection Act (hereinafter the Finnish DPA) complementing and specifying the regulation contained in the GDPR. The Parliament of Finland approved the government proposal for the new DPA HE 9/2018 vp on 13 November 2018. The Act came into effect on 1 January 2019. It is applicable in parallel to the GDPR and serves as a general law for personal data protection in Finland — available here (currently only in Finnish and Swedish):

https://valtioneuvosto.fi/delegate/file/49512

High-level overview of the key provisions of the National Data Protection Law

The new act repeals the old Finnish Personal Data Act (523/1999) as well as the Act on Data Protection Board and Data Protection Ombudsman (389/1994). The most essential provisions contained in the Finnish DPA are the following:

1. The Data Protection Ombudsman continues to act as the supervisory authority. The Office of the Data Protection Ombudsman shall have at least two Assistant Data Protection Ombudsmen as well as sufficient amount of other staff and reporting members who are acquainted with the operations of the Data Protection Ombudsman. As the Act on Data Protection Board and Data Protection Ombudsman is repealed, the current Data Protection Board has been abolished and instead, an expert board of five members is established in the context of the Office of the Data Protection Ombudsman. The expert board will adopt opinions regarding the application of the relevant regulations upon the request of the Data Protection Ombudsman.
2. The Data Protection Ombudsman can issue conditional fines to businesses, entities and authorities for the reinforcement of its data disclosure orders. The Data Protection Ombudsman together with the Assistant Data Protection Ombudsman will form a sanction collegium that is entitled to issue administrative fines in accordance with the GDPR. The ombudsman will act as the chair of the collegium. The collegium will have quorum with three members. The majority's decision will be adopted as the collegium's decision. The amount of the administrative fine can, in minor violations, be a maximum of EUR 10 million or 2% of the company's total turnover and, in violations that are more serious, the administrative fine can be a maximum of EUR 20 million or 4% of the total turnover. Administrative fines are not applicable to the processing of personal data in the public sector and in the Finnish Evangelical Lutheran or Eastern Orthodox Church.
3. Upon the approval of the Finnish DPA, the Finnish Parliament made a requirement according to which the Finnish Government is to examine whether the Data Protection Ombudsman's organization should be developed into a more office-like authority, and if needed, to prepare the necessary legislative amendments.
4. Data Protection offenses are criminalized under the Finnish Criminal Code (39/1889). The current provision in the Finnish Criminal Code on data protection offenses is, due to the legislative changes related to the GDPR, amended, and is as follows: A person who, as someone other than a controller or processor provided in the GDPR, intentionally or grossly negligently acquires personal data in a manner that is incompatible with the exclusivity of purpose, discloses personal data or transfers personal data in violation of the provisions of:
    i. the GDPR
    ii. the DPA
    iii. the Act on processing of personal data in criminal matters and in relation to the maintenance of national security
    iv. other Acts on data protection

    on the exclusivity of purpose, provisions on the disclosure and transfer, and thereby violates the privacy of the data subject or causes him or her other damage of significant inconvenience, shall be sentenced for a data protection offense to a fine or to imprisonment for at most one year.
5. Certain exemptions regarding the conditions for the processing of personal data with regard to, e.g., securing freedom of expression for journalistic purposes, were adopted in the Finnish DPA. Certain exemptions to the requirements of the GDPR were made with regard to scientific and historical research, statistics or archiving, if necessary for such purposes. Such exemptions include the data subject not having right of access in such cases. With this regard, the intention of the provisions is that the law remains as close as possible to the previous national legislation. Also, the processing of data concerning health, sexual behavior and orientation, religion and political views continues to be

possible for scientific and statistical purposes.

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

1. With regard to Article 8 GDPR, 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. Processing of data relating to criminal convictions and offenses shall be carried out only in the following situations:
    i. when necessary for solving, drafting, presenting, defending or resolving legal proceedings
    ii. if the data is processed by insurers where necessary for the determination of the liability of the insurer
    iii. where based on the provisions of an Act or necessary for compliance with an obligation to which the controller is subject directly by virtue of an Act
    iv. for purposes of scientific or historical research or the processing of data for statistical purposes

    Further provisions on privacy in the employment context are provided in the Act on the Protection of Privacy in Working Life, the Security Clearance Act, and the Act on Checking the Criminal Background of Persons Working with Children. As a rule, the employer has no right to carry out a background check on criminal records in the employment relationship. Exceptions to this are cases where the employment relationship involves work with minors or involves tasks related to the maintenance of the infrastructure critical for the functioning of society, such as energy, water and food supply and telecommunications, irrespective of whether they are performed in the public or private sector. In addition, the criminal background of employees manufacturing explosives and transporting valuable goods may be checked.

    The Security Clearance Act lays down provisions on the rights and status of the person or company subject to a security clearance. A person who will be subject to a security clearance must be informed of the clearance in advance, for example in the job advertisement. A clearance must not be carried out without consent of the person subject to the clearance. Similarly, a company must give its consent to a security clearance to be carried out regarding it.
3. The Finnish DPA and other Finnish legislation recognizes several situations in which the rights of a data subject may be restricted. The restrictions listed below are most relevant for commercial organizations.

    Restriction on right to information (Article 14 of the GDPR):

    Pursuant to the DPA, derogations from the information obligation based on Article 14 of the GDPR can be made where the provision of information causes material injury or harm to the data subject (e.g., situations where personal data relating to the data subject is used in a medical study on hereditary illnesses), and the relevant personal data is not used in decision-making regarding the data subject in question.

    Restrictions on right of access (Article 15 of the GDPR):

    The DPA provides a limited subset of grounds which can be relied upon to avoid disclosure of certain information in relation to a subject access request. Relevant grounds for commercial organizations are the following:

    i. where providing access to personal data could harm public order and security, or hinder the prevention or investigation of criminal offenses
    ii. where providing access to personal data could cause a serious risk to the health or treatment of the data subject, or to the rights of the data subject or of a third party

    Pursuant to the Finnish DPA, the data subject shall be informed of the reasons for the

restriction, unless this endangers the purpose of the restriction. In cases where the data subject has not been granted access to his or her personal data, the data subject may however request the controller to provide the data specified in Article 15(1) of the GDPR to the Data Protection Ombudsman.

Restrictions on right of access, right to rectification, right to restriction of processing and right to object (Article 15, 16, 18 and 21 of the GDPR):

The DPA provides limited possibilities to derogate from the rights of data subjects specified above, where personal data are processed for purposes of scientific or historical research, for statistical purposes or due to the right to freedom of expression and information. However, detailed preconditions apply.

4. There is a special legislation in force in the fields of healthcare and social welfare that requires each pharmacy and social welfare or healthcare service provider to appoint a DPO.

   In addition, the DPA defines certain special situations in which the entity must assess whether the appointment of a DPO is necessary. Appointment of a DPO is one of the safeguarding measures available to the entity, not a mandatory requirement in each of the situations mentioned in the DPA. It is the task of the entity in question to evaluate what safeguarding measures the risks involved in the processing require, and whether appointment of a DPO is necessary. The following circumstances in which the entity must assess the necessity to appoint a DPO are as follows:

   i. the entity is an insurance company processing special categories of personal data
   ii. the tasks of the entity that are laid down in the legislation necessitate the processing of special categories of personal data
   iii. the entity processes data that relates to a person belonging to a trade union and that is necessary in order for the entity to perform its rights and obligations on the field of employment law
   iv. the entity is a pharmacy, or a provider of social welfare or healthcare services
   v. the entity operates in the field of anti-doping or disabled persons, and the tasks of the entity necessitate the processing of genetic data or data concerning health
   vi. if the entity conducts scientific or historical research or compilations of statistics; and processes special categories of personal data for such purposes
   vii. if the entity processes scientific and cultural heritage related data that is not genetic data for non-profit archiving purposes

5. The Finnish DPA does not set any further limits on the transfer of special categories of personal data to third countries or international organizations than provided in the GDPR.

6. The Finnish DPA provides that a personal identification number may be processed on the unambiguous consent of the data subject or where so provided by law. A personal identification number may also be processed if it is necessary to unambiguously identify the data subject:

   i. in order to perform a tasks laid down by law
   ii. in order to realize the rights or duties of the data subject or the controller
   iii. for purposes of historical, scientific or statistical research

   A personal identification may be processed in activities relating to the granting of credit and the collection of debt, in the insurance, credit, payment, renting and lending businesses, in credit data operations, in healthcare, in social welfare activities or other social services and in matters relating to the civil service, employment and other service relationships and benefits to the same.

   In addition, a personal identification number may be disclosed for the purposes of updating of address information and prevention of redundant postal traffic, provided that the personal identification number is already available to the recipient.

	The controller shall see to that the personal identification number is not unnecessarily included in hard copies printed or drawn up from the personal data file. 7. For the protection of personal data processed in connection with scientific and historical research and statistical purposes, the Finnish DPA requires that a data protection impact assessment is conducted and a written notification is submitted to the Data Protection Ombudsman before processing if there is a need to deviate from the data subject rights under the GDPR. The deviation from the data subject rights under the GDPR requires also that: i. the processing is based on an appropriate research plan ii. there is a responsible person or group of the research iii. personal data is processed or disclosed only for the purposes of historical or scientific research, or other similar purposes and the operations are conducted in such a manner that third parties do not become aware of the personal data regarding a specific person
France	Links to the National Data Protection Law On 20 June 2018, the bill on the protection of personal data (the French Data Protection Act 2 or "FDPA 2") was officially enacted. The law is available here: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460 The FDP2 has been completed by: 1. Decree of 1 August 2018 https://www.legifrance.gouv.fr/eli/decret/2018/8/1/JUSC1815709D/jo/texte 2. Executive Order of 12 December 2018 https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=344F3A0F747E4E780A381147E0E8C922.tplgfr27s_2?cidTexte=JORFTEXT000037800506&dateTexte=&oldAction=rechJO&categorieLien=id&idJO=JORFCONT000037800456 Please note that the executive order has entirely redrafted the FDPA and will enter into force on 1 June 2019 at the latest. Due to the date of the publication of the present study, the executive order has not been taken into account. High-level overview of the key provisions of the National Data Protection Law 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 — the French Supervisory Authority) with the philosophy introduced by the GDPR of enhanced accountability of stakeholders. The most important subject matters covered by the FDPA 2 are: **1. 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. **2. 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 heath data

ii. in the public sector

iii. until the entry into force of the Executive Order dated 12 December 2018, for data processing carried out by data controllers in the following French overseas territories: New Caledonia, Wallis and Futuna, French Polynesia, French Southern and Antarctic Lands.

3. The definition of the age for "digital majority" (Article 70):

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.

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

1. Article 8 GDPR (age of minor consent)

The age of consent is 15 years.

2. Article 10 GDPR (processing of data relating to criminal convictions and offenses especially in the employment relationship)

Internal investigations, processing of data relating to criminal convictions and offenses may only be processed by a restricted list of controllers. The list is provided by Article 9 of the French Data Protection Act 2, June 2018 ("FDPA 2") including courts, public authorities and legal entities managing public services as part of their statutory missions or court officers.

3. Article 23 GDPR (relevant restrictions on data subject rights)

Data subject rights are restricted when it concerns state security, public defense or public security. The data subject right to access shall be addressed to the CNIL which appoints one of its members to carry out the necessary investigations and authorize the access or not (Article 41 of the FDPA 2).

Moreover, the part of the FDPA 2 which transposes the Directive "Police-Justice" imposes restriction of the data subject rights, in order to:

i. avoid affecting the progress of an investigation, researches, administrative or judicial proceedings

ii. avoid affecting the prevention or detection of criminal offenses, investigations or prosecution related to criminal sanctions

iii. protect public security

iv. protect national security

v. protect the rights and freedoms of others

If one of the condition aforementioned is met, the controller may:

i. delay or not communicate the information

ii. refuse or limit the right of access of the person

iii. not inform the data subject of the refusal to rectify or delete his or her personal data

These restrictions must constitute a necessary and proportionate measure in a democratic society, taking into account the fundamental rights and legitimate interests of individuals (Article 70-21 of the FDPA 2).

4. Article 37(4) GDPR (additional thresholds requiring the appointment of a DPO)

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.

	5. Article 87 GDPR (specific rules for the processing of national IDs) Processing of national IDs is subject to specific requirements determined by a decree of the French Conseil d'Etat which details the categories of controller and the purposes of processing. Please note, that such decree has not yet been issued. The restriction does not apply to the following purposes: i. statistical purpose implemented by the national statistical service and its process exclude sensitive data or data relating to criminal offenses ii. exclusively scientific or historical purpose or for supplying users with one or more online government services, under certain conditions **6. Any requirements for filings and/or notifications with the national data protection authority** The FDPA 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) ii. for health data iii. in the public sector iv. for data processing carried out by data controllers in the following French overseas territories until the Executive Order of 12 December 2018 comes into force: New Caledonia, Wallis and Futuna, French Polynesia, French Southern and Antarctic Lands
Germany	Link to the National Data Protection Law In May 2017, Germany passed a bill that revoked the existing Federal Data Protection Law, which has been in force for the last 40 years, and enacted a new national data protection law supplementing the GDPR ("Federal Data Protection Act" or "FDPA") — available here: https://dejure.org/gesetze/BDSG Sector-specific privacy acts have also been or shall be amended in light of GDPR, such as the hospital laws, the Social Act (primarily relevant for data processing in the context of health insurance and by public bodies), national security acts, pharma laws, laws protection public health, etc. High-level overview of the key provisions of the National Data Protection Law The most important subject matters covered by the FDPA are: **1. Additional thresholds for DPOs (see below)** **2. Specifications for the processing of sensitive data pursuant to Art. 9 GDPR** The FDPA 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: i. if the processing is necessary to exercise rights and comply with obligations in the area of social security or social protection laws ii. 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 iii. for reasons of public interest in the area of public health, such as protection against severe cross-border health risks iv. for archiving purposes in the public interest, or for scientific or historical research purposes

3. **Rules for the processing of employee data**

   Comprehensive rules on data protection in an employment context have been established. Those rules are seemingly built on the rules under the old FDPA, as well as the rules and legal opinions formed by German legal literature, courts and DPAs. According to Sec. 26, personal data of employees may be processed for employment purposes or to reveal a criminal offense. Further, the FDPA specifies when the consent of an employee is deemed freely given and valid and when the processing of special categories of data is permitted in an employment context, e.g., 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.

4. **Scoring and credit checks**

   According to Sec. 31 FDPA, the use of scoring and credit checks underlies certain requirements and may only be used if privacy rules are met, if relevant data are used and if the score is based on acknowledged, reliable mathematical-statistical methods. It is not allowed to determine a score solely based on address data because the law requires information of the data subject in the case of using address data.

5. **Potential criminal liability in case of certain violations of the GDPR**

6. **Restrictions for data subject rights (see below)**

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

The German legislature has made extensive use of the opener clauses.

1. **Age of minors for consent (Art. 8 GDPR)**

   The age of minors for consent remains at 16 years.

2. **Processing of data relating to criminal convictions and offenses (Article 10 GDPR)**

   There is no explicit provision in the FDPA referring to Art. 10 GDPR.

   However, employees' personal data may be processed to detect crimes only if there is a documented reason to believe the data subject has committed a crime while employed, the processing of such data is necessary to investigate the crime and is not outweighed by the data subject's legitimate interest in not processing the data, and in particular the type and extent are not disproportionate to the reason.

   It is unclear whether Art. 10 GDPR applies also in case of suspected criminal activity which may be processed in the context of whistleblowing hotlines, internal investigations or background screenings. Given recent statements of the German data protection authorities relating to whistleblowing hotlines, it seems like the authorities do not consider Art. 10 GDPR applicable for the data processing relating to whistleblowing, i.e., to the processing of suspected criminal offenses.

3. **Data subject rights**

   The German FDPA provides for several restrictions of data subject rights based on Art. 23 GDPR. However, several of the restrictions are currently being debated as to whether or not they are in compliance with GDPR and the framework for restrictions set out in Art. 23 GDPR:

   i. In case of processing for scientific or historical research or statistical purposes, data subject rights pursuant to Art. 15, 16, 18 and 21 GDPR shall be limited to the extent that these rights are likely to render impossible or seriously impair the achievement of the scientific or historical research or statistical purposes; the access right pursuant to Art. 15 GDPR shall not apply in case of scientific research if access to the data would involve disproportionate efforts.

   ii. In case of processing for archiving purposes in the public interest, Article 15 GDPR shall not apply if the archived data is not identified with the person's name or if the identification of the data would require unreasonable administrative efforts and

Article 16 GDPR shall not apply at all, however, the data subject may request that his or her corrections are added to the archived file, and certain rights under Art. 18, 20, and 21 GDPR shall not apply if they likely render impossible or seriously impair the achievement of the archiving purpose.

iii. Art. 13 (3) GDPR relating to information about the intended secondary processing purposes is restricted in certain circumstances, such as interference with the establishment, or exercise or defense of legal claims, in which case the controller must provide such information typically to the public.

iv. Art. 13 (3) GDPR is restricted where personal data is transferred to a lawyer in the context of an attorney-client relationship.

v. Art. 14 (1) to (4) GDPR shall not apply as far as meeting this obligation would disclose information which by its nature must be kept secret, in particular because of overriding legitimate interests of a third party.

vi. Art. 14 (1), (2) and (4) GDPR may not apply for private bodies where meeting this obligation would interfere with the establishment, exercise or defense of legal claims, or processing includes data from contracts under private law and is intended to prevent harm from criminal offenses, or where disclosing the data would endanger public security, in which case the controller must provide such information typically to the public.

vii. Art. 15 GDPR shall not apply: (i) as far as access would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party; (ii) where disclosing the data would endanger public security; (iii) where the data is retained only for purposes of compliance with legal or statutory retention requirements; or (iv) where the data is processed only for purposes of monitoring data protection, and in cases (iii) and (iv), providing the information would require a disproportionate effort and appropriate technical and organizational measures make processing for other purposes impossible.

viii. Art. 17 GDPR shall not apply in case of lawful non-automated processing where the deletion is impossible or requires a disproportionate effort due to the specific type of storage and the interests of the data subject are rather low. In this case, further processing must be restricted.

ix. Art. 17 para. 1 (a) and (d) GDPR shall not apply, as long and as far as the controller has reason to believe that erasure would adversely affect legitimate interests of the data subject.

x. Art. 34 GDPR (obligation to inform a data subject of a personal data breach) shall not apply as far as meeting this obligation would disclose information which by law or by its nature must be kept secret, in particular because of overriding legitimate interests of a third party, unless the interests of the data subject outweigh the interest in secrecy, in particular taking into account the threat of damage.

4. Data protection officer

The German rules regarding the duty to appoint a DPO are stricter than those stipulated by Article 37 GDPR: The FDPA 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 where they commercially process personal data for the purpose of (anonymous) transfer or for purposes of market or opinion research, as well as if a DPIA pursuant to Article 35 GDPR is required.

5. Restrictions on the transfer of sensitive data to third countries without an adequacy decision (Article 49 (5) GDPR)

There are no general restrictions in the German Federal Data Protection Act. However, sector-specific privacy laws such as for hospitals and for bodies falling under the Social Act (particularly relevant for health insurance companies) provide for restrictions on international data transfer of sensitive data.

	6. Specific rules for the processing of national IDs (Article 87 GDPR) There are no specific rules on this issue in the German FDPA, but the Passport Act imposes restrictions relating to copies of ID cards and passports. **7. Any requirements for filings and/or notifications with the national data protection authority** There are no filing and/or notifications with the national data protection authority beyond those in the GDPR.
Greece	N/A — no adopted National Data Protection Law yet
Hungary	Link to the National Data Protection Law On 17 July 2018, the Hungarian Parliament adopted Act XXXVIII of 2018, the Hungarian national law supplementing the GDPR ("Amendment") and amending Act No. CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information ("Information Act") — available here: https://net.jogtar.hu/jogszabaly?docid=A1100112.TV High-level overview of the key provisions of the National Data Protection Law 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 data processing operation(s) relate(s) to: - the offering of goods or services to data subjects located in Hungary, irrespective of whether a payment by the data subject is required - 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. 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.

6. **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.

7. **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.

8. **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 wide range of persons or the activity of a state budget authority
   - the gravity of the infringement justifies publication of the decision

ii. The fine that may be imposed on a state budget authority is capped at a maximum of HUF 20 million (approx. EUR 60,000).

9. **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.

10. **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.

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

1. **Digital age of consent**

The age of consent relative to information society services remains 16 years of age under the Amendment.

2. **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 (pursuant to Section 5(7) of the Information Act). 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.

3. **Data Protection Officer (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. 4. Section 28 of the Act XXI of 2008 on the protection of human genetic data, imposes a notification obligation to Hungary's Chief Public Health Officer in connection with the international transfer of genetic data and genetic samples for the purpose of human genetic research and human genetic testing. That notification must contain a reference to the appropriate adequacy safeguards provided by the exporter/importer. 5. The Act XX of 1996 on the methods of identification replacing the personal identification number, and the use of identification codes regulates the use of the tax ID, national identification number and the social security ID. These IDs may be processed only if there is a legal obligation to process this data or if the data subject has granted its written (i.e., wet signature) consent to the data processing. The legislation says that the data subject may not receive any benefits/rewards in connection with granting the consent. 6. Sections 156 (2)-(8) of the Act C of 2003 on Electronic Communications establish a personal data breach notification obligation for providers of public electronic communication services to the Hungarian Media and Infocommunication Authority (NMHH) if the personal data of telecom services subscribers or users is breached. NMHH Decree No. 4/2012 (I.24.) establishes the details of the data breach notification obligation. If a personal data breach occurs, the provider of public electronic communication services must, without undue delay, but, in any case, within 24 hours, notify the NMHH of that breach. After the first notification is made, the telecom service provider must gather the information necessary for the second notification, which must be submitted without undue delay, but no later than 72 hours from the first notification. Until the closure of its investigation, the telecom service provider must update the NMHH monthly on information arising from its investigation in the past month.
Ireland	Link to the National Data Protection Law The Irish Data Protection Act 2018 ("2018 Act") was signed into law on 24 May 2018 to supplement the GDPR. It is available here: http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html High-level overview of the key provisions of the National Data Protection Law The 2018 Act 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: 1. setting the digital age of consent at 16 years 2. 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) 3. providing restrictions on individuals' rights and controllers' obligations on the grounds of legal privilege 4. archiving, scientific or historical research or statistical purposes 5. freedom of expression and in other specified circumstances for the importance objective of public interest 6. 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 7. 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

8. providing a lawful basis for the processing of health data for insurance and pension purposes or the mortgaging of property

9. 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

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

1. Article 10 GDPR (processing of data relating to criminal convictions and offenses especially in the employment relationship)

i. The 2018 Act (section 55(1)) permits the processing of Article 10 data (i.e., personal data relating to criminal convictions and offenses) in specified circumstances, including:

- with the explicit consent of the data subject
- where the processing is necessary and proportionate for the performance of a contract to which the data subject is a party
- where necessary for the purpose of legal advice, legal claims, legal proceedings, or exercising or defending legal claims
- where necessary to prevent injury or other damage to the data subject or another person or loss or damage to property, or to protect the vital interests of the data subject
- where permitted by Ministerial regulations or other Irish law.

ii. Section 55(2) further permits the processing of Article 10 data under the control of official authority, including for the following purposes:

- the administration of justice
- the exercise of a regulatory, authorizing or licensing function or determination of eligibility for benefits or services
- protection of the public against harm arising from dishonesty, malpractice, breaches of ethics or other improper conduct by, or the unfitness or incompetence of, persons who are or were authorised to carry on a profession or other activity
- enforcement actions aimed at preventing, detecting or investigating breaches of EU or Irish law that are subject to civil or administrative sanctions
- archiving in the public interest, scientific or historical research purposes or statistical purposes where the processing is carried out by or on behalf of a public authority or public body

These provisions are without prejudice to the provisions of the Criminal Justice (Spent Convictions and Certain Disclosures) Act 2016, and subject to compliance with Article 6(1) (i.e., having a lawful basis) and to suitable and specific measures being taken to safeguard data subject rights.

It is an offense to knowingly or recklessly process personal data relating to criminal convictions and offenses in contravention of section 55, punishable by a fine up to EUR 50,000 and/or imprisonment for up to five years.

2. Article 23 GDPR (relevant restrictions on data subject rights)

i. The 2018 Act (section 60(3)) provides that individuals' rights provided for in Articles 12 to 22 of the GDPR and Article 34, and the obligations of controllers in Article 5 may be restricted where necessary and proportionate:

- to safeguard cabinet confidentiality, judicial independence and court proceedings, parliamentary privilege, national security, defense and the

	international relations of the state (section 60(3)(a)(i)) - for the prevention, detection, investigation and prosecution of criminal offenses and the execution of criminal penalties (section 60(3)(a)(ii)) - for the administration of any tax, duty or other money due or owing to the State or a local authority in any case in which the non-application of the restrictions concerned would be likely to prejudice such administration (section 60(3)(a)(iii)) - for the exercise or defense of legal claims or legal proceedings whether before a court, statutory tribunal, statutory body or an administrative or out-of-court procedure (section 60(3)(a)(iv)) - for the enforcement of civil law claims, including matters relating to any liability of a controller or processor in respect of damages, compensation or other liabilities or debts related to the claim (section 60(3)(a)(v)) - for the purposes of estimating the liability of a controller for damages on foot of a claim for the payment of a sum of money, in any case in which the application of those rights or obligations would be likely to prejudice the interests of the controller (section 60(3)(a)(vi)) - where the personal data relates to an expression of opinion about the data subject given in confidence or on the understanding that it would be treated as confidential to a person who has a legitimate interest in receiving the information (section 60(3)(b)) - where the information is protected by legal privilege (section 162) iii. In addition, where processing is for archiving purposes in the public interest or for scientific or historical research or statistical purposes, certain rights of a data subject may be restricted to the extent that the exercise of those rights would be likely to render impossible, or seriously impair, the achievement of those purposes, and such restriction is necessary for the fulfilment of those purposes (section 61). iv. An individual's right under Article 15 to obtain a copy of his/her personal data may be further restricted where: - in the opinion of a health practitioner, the supply of health data would cause serious harm to his or her physical or mental health (section 68(2)(a)) - the supply of social work data (including personal data obtained in the course of social work carried out by a public authority, public body, voluntary organization or other body), would cause serious harm to the health or emotional condition of the data subject concerned (section 68(3))
Italy	Link to the National Data Protection Law On 8 August 2018, the Council of Ministers approved the decree of GDPR harmonization, and on 4 September 2018 the Legislative Decree no. 101/2018 was passed — available here: http:www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=2018-09-04&atto.codiceRedazionale=18G00129&elenco30giorni=false High-level overview of the key provisions of the National Data Protection Law **The Italian way of the GDPR** The Legislative Decree of 10 August 2018, n. 101, ("Alignment Decree"), has aligned the Italian privacy law to the GDPR, applicable as of 25 May 2018. Notwithstanding the fact that this is a Regulation, and as such it is immediately applicable in Member States, the GDPR provides for some opening clauses that allow the national legislator to intervene in specific matters — for example the Regulation requires the appointment of a DPO (Data Protection Officer) in certain cases, leaving to Member States the possibility to identify further cases when such appointment is necessary. The journey of the Alignment Decree started with the Law of 25 October 2017, n. 163 , i.e.,

the European delegation law 2016-2017, which required the government to align Italian privacy law with the GDPR, through prior consultation with the Italian data protection authority (the "Garante"). The Alignment Decree was eventually published in the Official Gazette on 4 September 2018 and entered into force on 19 September 2018.

The new Privacy Code

To align Italian privacy law with the GDPR, the government repealed and amended the relevant provisions of the "old" Italian Privacy Code (Legislative Decree 196/2003, consolidated version) in order to make them consistent with the GDPR, and revised in the same way the other applicable data protection provisions. The Garante has the ability to adopt specific provisions in this direction.

A first comment on the new Privacy Code, which represents (with the GDPR) the main legislative reference for companies and operators, is that the same is not an easy text for consultation and use, since there are a number of cross-references among the articles of the same Privacy Code, the GDPR and other pieces of law.

Hereinafter we identify the matters that, at first reading, deserve immediate attention.

Eight months for the first application phase and simplified conditions for SMEs

The last part of the Alignment Decree reports that for eight months from its entering into force, the Garante will take into account "the first application phase *[….] for purpose of application of administrative fines*." The GDPR and (from 19 September) the Alignment Decree are therefore valid and in force, meaning the Garante has opted for more than a suspension or grace period. This is to be intended as an important and welcome indication of reasonableness in application, considering the complexity of the relevant legislative framework as drawn up by the GDPR and refined by the Alignment Decree. Therefore, an approach shall be considered viable as long as it is in line with the GDPR.

The choice of adopting a reasonable and good-sense approach, instead of granting a grace period, had already been put forward by the Garante in the Provision issued last February in relation to some elements of the Budget Act (*Legge di Bilancio*) 2018, that among others had requested the Garante to adopt guidelines or best practices to help companies in making use of the legitimate interest right as a legal basis for data processing. The Provision was also aimed at providing some indications in light of the deadline of 25 May. Therefore the Garante, taking into account the fact that the legislative measures to align Italian privacy law to the GDPR had not yet been issued and that this alignment might have a *profound* regulatory impact, decided to extend the application of the Provision to six months as of entering into force of the Alignment Decree. This time period also enabled the Garante to interact with relevant stakeholders.

The Alignment Decree also provides that the Garante shall act to identify simplified measures for GDPR implementation for the benefit of small and medium enterprises.

Codes of conduct, general authorization of the Garante and powers of the Garante

The codes of conduct contained in Annex A of the "old" Privacy Code (listed in sequence numbering, thus A I, A II, etc.) will be evaluated by the Garante within three months as of entering into force of the Alignment Decree to assess their coherence with the GDPR. The codes that will be deemed as GDPR compliant, renamed the "*rules of professional conduct*", will be published in the Official Gazette and inserted as Annex A to the "new" Privacy Code. The current codes of conduct relate to information systems managed by private entities in relation to consumer credit, reliability and timeliness in payments as well as the processing of personal data for commercial information purposes (respectively, Annex A 5 and A 7 of the Privacy Code). These codes will remain applicable until the end of the approval procedure of the codes of conduct as introduced by the GDPR. Within six months the associations and representative bodies of stakeholders should submit the revised codes to the Garante, which will examine the same within the following six months. If the above-identified deadlines are not met, the codes will be repealed.

As for the general authorizations of the Garante, within three months the same will issue a general provision identifying or, as the case may be, updating the parts of said authorizations that will remain applicable as in line with the GDPR and the new Privacy Code, following a

public consultation. It should be noted that a breach of the to-be-determined general authorizations triggers the application of the higher threshold of the administrative fines, notably EUR 20 million or, if higher, 4% of the total worldwide turnover, in case of undertaking.

The Garante may propose the adoption of rules of professional practice for the processing of genetic, biometric, or health-related data, data processing within the employment relationship, or data relating to scientific or historical research, processing for the coordination of freedom of expression and information, as well as for data processing that is necessary to comply with a legal obligation.

This is an important corrective element to the complexity of the regulatory framework resulting from the new Privacy Code, which allows the Garante and stakeholders to fine tune the law requirements to the specific needs and factual circumstances of the involved stakeholders.

As allowed by the GDPR, the Alignment Decree has granted to the Garante further powers, specifically: The power to adopt guidelines on the organizational and technical measures to implement the GDPR and the power to approve the rules of professional conduct. The Garante may also ask the personnel of foreign Member States' privacy supervisory authorities to participate in its auditing activities.

Lastly, the provisions of the Garante issued before 25 May and, more generally, the current provisions on data protection will remain applicable as far as they are in line with the GDPR and the Alignment Decree and shall be interpreted according to the same, namely guaranteeing coherence and stability in the legislative benchmark.

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

Special categories of data and consent of minors

Genetic, biometric and health data may not be disclosed and the Garante, at least every two years, will identify the specific measures and conditions for their lawful processing. For genetic data, in case of high risk, it is envisaged that such measures and conditions may also include the consent requirements or other specific protective measures. It is expressly allowed, under specific circumstances, the use of biometric data to grant physical and logical access to data.

The processing of so-called judicial data, notably data relating to criminal convictions and offenses, must be allowed by law, regulation or, in the absence of the same, by a decree of the Ministry of Justice issued with prior consultation with the Garante. In the description of the applicable rules there is express reference to the possibility of processing such data, under specific conditions: within tenders, whilst awarding the legality rating of companies and within the employment relationship. The latter must be within the limitations set forth by laws, regulations and collective agreements.

In relation to offering information society services directly to a child, the age of minors to provide a valid consent is established at 14 years (16 years under the GDPR, save different provisions of national legislation). It is necessary to inform minors on how and why data is processed in a simple and comprehensible way.

The privacy rights of data subjects and deceased persons

With regard to the privacy rights of the data subjects, which have been significantly extended and reinforced by the GDPR, the Alignment Decree identifies some limitations to their enforcement, such as in the case of defensive investigations, the enforcement of rights in judicial cases and the protection of the confidentiality of the employee who files a report under a whistleblowing scheme set up as provided under the law. When data subject rights may be compressed, companies can revert to the Garante for their enforcement and must inform thereon the data subjects. It is thus necessary to consequently update the applicable privacy notices in order to capture this case.

For the personal data of deceased persons, the Alignment Decree recognizes that the relevant privacy rights (for example access, deletion, etc.) may be enforced by a person who acts in the interest of the deceased person or by a person who has his/her own interest as

	proxy or for family reasons deserving protection. Within the digital environment, the person may prohibit the enforcement of his/her privacy rights expressly through written statement that is express, specific, free and informed, being it understood that the possibility to prohibit cannot prejudice the enforcement of property rights or the right to defend one's own interests. **Internal privacy delegation system** Companies may delegate internally specific duties and activities relating to privacy, and the Alignment Decree also provides for the possibility for companies to identify the preferred conditions to authorize the personnel to process data, in order to grant them a certain degree of discretion in defining their own privacy structure and the way to adopt their own privacy organizational model. **Consent for scientific research** The previous rule on the consent of the data subject for scientific research purposes is modified as follows: Consent is not necessary when the research is carried out according to laws, regulations or Union legislation, but it is necessary to perform and make public a data protection impact assessment according to the GDPR. Furthermore, consent is not required when informing data subjects is impossible or requires a disproportionate effort, or may render impossible or provide serious prejudice to the fulfillment of the research results. In these cases, the previous authorization of the Garante is replaced with the prior consultation of the same according to the GDPR. Under specific circumstances, the Garante may authorize, for scientific research and statistical purposes, the further processing of health data, without the delivery of privacy notices to the data subjects. **Notification to the Garante** The Alignment Decree does not entail filings/notification requirements, however, the Budget Act 2018 introduced an obligation to communicate to the Garante all processing based on a legitimate interest, according to a specific form that must be published on the website of the Garante. After 15 days, in case of no response from the Garante, the controller can start the processing, with the caveat that the Garante has the possibility to stop the processing for 30 days in order to ask for further information and provide a decision on the processing. This procedure has been held by the Garante to be in contrast with the GDPR, and specifically the accountability principle, so the Italian GDPR alignment law has limited the above procedure of communication to the Garante of any processing based on legitimate interest to very specific cases, notably when the processing is necessary to effect a change of name or surname of minors, thus limiting the procedure to performance of public interest tasks that may present high risk. The Garante may adopt general orders to rule more specifically on this matter. **The criminal sanctioning system** The criminal sanctioning system is confirmed under the Alignment Decree, with some amendments and more text dedicated to criminal conducts. Specifically, when a large number of persons is involved, the Alignment Decree introduces the criminal sanction of imprisonment for up to six years for the unlawful communication and disclosure of data residing on an automated archive, and up to four years for the unlawful acquisition of an automated archive. Furthermore, for the interruption or disturbance of the auditing activities of, or proceedings in front of, the Garante, a sanction of up to one year's imprisonment has been introduced.
Latvia	Link to the National Data Protection Law The Personal Data Processing Law in Latvia entered into force on 5 July 2018: https://likumi.lv/ta/en/en/id/300099-personal-data-processing-law High-level overview of the key provisions of the National Data Protection Law The new Personal Data Processing Law replaced the Law on the Protection of Personal Data of Natural Persons of 2000 and made Latvia the first Baltic state that adopted its own national legislation based on the GDPR. The 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. The law includes exemptions from the general rules regarding data processing for journalistic, academic and literary purposes, freedom of expression, archiving purposes in the public interest, and scientific, historical research or statistical purposes in accordance with Article 89 of the GDPR. Additionally, data processing in official publications is exemption from the general rules. Also, among other provision, the Latvian Data Processing Law implements that civil claim arising out of violation of the GDPR obligations can be initiated within a period of five years from the moment of infringement occurred or from the day when the infringement has stopped (limitation period for other civil claims is 10 years). Details on how the National Data Protection Law made use of specific opener clauses of the GDPR 1. Under the Latvian Data Processing Law, the age from which a data subject can provide its consent in relation to data processing by information society services is 13 years. 2. The processing of data relating to criminal convictions and offenses is not specifically regulated by National Data Protection Law. However, the Latvian Employment law does forbid the processing of such data (for example, for background checks) except if it is required under respective laws or regulations regulating specific professions such as teachers, civil servants and others. 3. The national Data Processing Law includes a limitation for data subject access requests. The data subject does not have the right to receive the information specified in Article 15 of the GDPR if it is prohibited to disclose such information in accordance with the laws and regulations regarding national security, national protection, public safety and criminal law, as well as for the purpose of ensuring public financial interests in the areas of tax protection, prevention of money laundering and terrorism financing or of ensuring of supervision of financial market participants and functioning of guarantee systems thereof, application of regulation and macroeconomic analysis. Furthermore, the law provides a possibility to restrict additional data subject rights provided in other laws and regulations in accordance with Article 23 of the GDPR. 4. Regarding the notification requirements with the national data protection authority, the data controllers or processors in accordance with Article 37 (7) of the GDPR must within three days notify Latvian Data Protection Authority (Data State Inspectorate) regarding the designation of a data protection authority. There are no additional thresholds requiring the designation of Data Protection Officers. 5. Latvian legislation has not implemented any provisions for restrictions on the transfer of sensitive data to third countries without an adequacy decision, there are no longer any specific rules for the processing of national IDs.
Lithuania	Link to the National Data Protection Law On 16 July 2018, the new Law on Legal Data Protection of Personal Data of the Republic of Lithuania came into force — available here: https://www.e-tar.lt/portal/lt/legalAct/TAR.5368B592234C/VCRurdZydD High-level overview of the key provisions of the National Data Protection Law 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 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. Details on how the National Data Protection Law made use of specific opener clauses of the GDPR **1. Digital age of consent** 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. **2. Criminal conviction data processing** It is prohibited to process employee's or candidate's personal data related to criminal convictions or offenses (unless required by law). **3. Nation ID processing** It is forbidden to publish data subject's personal code or to process it for direct marketing purposes.
Luxembourg	Link to the National Data Protection Law 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 — available here: http://data.legilux.public.lu/file/eli-etat-leg-loi-2018-08-01-a686-jo-fr-pdf.pdf High-level overview of the key provisions of the National Data Protection Law 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:

1. 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)
2. have legal standing and initiate judicial proceedings in the interests of the GDPR
3. require from any data controller or processor all the necessary information to assess their compliance with the GDPR
4. order a data controller/processor to suspend or stop the processing of personal data
5. 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:

1. 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).
2. 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.

    Such information must consist of a detailed description of the purposes of the processing, the modalities of the monitoring system and the period for which the data will be stored (or if that is not possible, the criteria used to determine that period), and contain a formal declaration by the employer that he/she will not use the personal data for any other purposes than those explicitly mentioned. This information is without prejudice to the employees' general right to be informed under Article 13 of the GDPR. Within 15 days of receipt of such prior information, the staff delegation, or in the absence thereof, the concerned employees, may request a prior opinion on the monitoring project with the CNPD. Such request has a suspensive effect so that the monitoring project cannot be implemented before the CNPD has handed down its opinion. The CNPD should deliver its opinion within the month (also new article L. 261-1 of the Employment 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. Details on how the National Data Protection Law made use of specific opener clauses of the GDPR Luxembourg has very limitedly made us of specific opener clause of the GDPR: 1. processing and freedom of expression and information 2. processing for scientific or historical research purposes or statistical purposes 3. processing of genetic data for the purpose of the exercise of the rights of the controller in the area of labor law and insurance is prohibited
Malta	Link to the National Data Protection Law The Maltese Data Protection Act (Chapter 440 of the Laws of Malta) ("DPA") was repealed by the new Act No. XX of 2018, which was adopted on 28 May 2018 — available here: http://justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8906&l=1 High-level overview of the key provisions of the National Data Protection Law 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 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. Details on how the National Data Protection Law made use of specific opener clauses of the GDPR The age of minor consent has been lowered to 13.
Netherlands	Link to the National Data Protection Law The Dutch GDPR Implementation Act which serves to supplement the GDPR ("UAVG") was published in the Netherlands' Official Bulletin of Acts and Decrees (Staatsblad 2018 144) on 16 May 2018. The official text, including all national particularities, is available (in Dutch only) at: https://www.officielebekendmakingen.nl/stb-2018-144.pdf High-level overview of the key provisions of the National Data Protection Law 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. Details on how the National Data Protection Law made use of specific opener clauses of the GDPR Some notable provisions relate to:

	1. Age of minors (Art. 8 GDPR) The age of minors for consent is 16. **2. Processing of data relating to criminal convictions and offenses (Art. 10 GDPR)** General and specific exemptions apply to the prohibition to process data related to criminal behavior, for example if it is: a. carried out with the data subject's explicit consent for the processing of personal data for one or more specified purposes b. necessary to protect the vital interests of the data subject or of another natural person if the data subject is physically or legally incapable of giving consent c. related to personal data which are manifestly made public by the data subject d. necessary for the establishment, exercise or defense of legal claims or when courts are acting in their judicial capacity e. necessary for reasons of substantial public interest as referred to in article 23 (a) and (b) GDPR f. necessary for scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) of the GDPR g. carried out by bodies that are responsible for applying criminal law pursuant to the Police Data Act or the Judicial Data and Criminal Records Act h. carried out by and on behalf of alliances of controllers or groups of controllers governed by public law i. necessary for the proper treatment or care of the person concerned j. necessary to assess a request from the data subject to take a decision providing services to him or her k. necessary to protect the controller's interests in cases of criminal offenses committed against him or which, on the basis of facts and circumstances, can be expected to be committed against him/her or persons employed by him/her l. carried out for the benefit of a third party by a controller acting pursuant to a license under the Private Security Organizations and Detective Agencies Act or having a license granted by the Dutch DPA **3. Data subject rights** An exception to the data subject rights exists in the interest of public registries. **4. Data protection officer** The Dutch legislator has not made use of the possibility of additional thresholds. **5. Restrictions on the transfer of sensitive data to third countries without an adequacy decision (Art. 49 (5) GDPR)** The Dutch legislator has not made use of this possibility in the UAVG. Specific derogations may be implemented in (sector) specific legislation. **6. Specific rules for the processing of national IDs (Art 87 GDPR)** The processing of a social security number (which is printed on different national IDs) is prohibited in the absence of a statutory obligation to process it. **7. Any requirements for filings and/or notifications with the national data protection authority** Under the former Dutch Personal Data Protection Act, there was a data processing notification requirement. Under the GDPR, such notification obligation no longer exists.
Poland	Link to the National Data Protection Law

The new Act of 10 May 2018 on Personal Data Protection ("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. It is available at:

http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001000/U/D20181000Lj.pdf

High-level overview of the key provisions of the National Data Protection Law

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 became 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.

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.

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

1. Poland has not adopted any general laws allowing data controllers to process data pertaining to criminal convictions and offenses. So far only certain sectoral laws have been adopted in this area. The most relevant example is the Act of 12 April 2018 on the Principles of Obtaining Information about the Criminal Record of Candidates Applying for Employment and Persons Employed in Entities from the Financial Sector which allows employers from the this sector (e.g., banks, insurers or entities providing certain services to financial institutions), to conduct limited employee criminal background checks. However, this exception applies only to employees or candidates for positions that are connected with managing of assets, access to confidential information, making decisions that may be subject to a risk of losing the assets or causing a material damage to the employer or a third party.
2. Furthermore, Poland has adopted the Act of 10 May 2018 on Personal Data Protection according to which the rights listed in Articles 15 to 16 and 18 to 22 GDPR do not apply to any activity which consists of editing, preparing, creating or publishing press materials within the meaning of the Act of 26 January 1984 on Press Law, as well as to literary or artistic expression. Moreover, the right to demand a copy of data being processed (Art. 15 para. 3 and 4 GDPR), as well as the right to restriction of processing, do not apply to the processing of personal data for the purposes of academic expression.

   The data subject's right to access personal data (Article 15 para. 1 to 3 GDPR) has been additionally restricted in case of controllers performing public tasks, if such restriction serves the purpose of performing a public task, provided that certain additional conditions have been met. Instead, the controller must provide appropriate measures to

	protect the interests or fundamental rights and freedoms of the data subject. Moreover, the data subject must be informed, without undue delay, but no later that within one month from the date of receipt of the request, of the grounds for non-performance of the obligations referred to above. Additionally, where the performance of the obligations resulting from the access right involves a disproportionate effort connected with the retrieval of personal data, the controller performing a public task may ask the data subject to specify its demand and provide the information allowing retrieval of those data. 3. According to the PDPA the DPO notification must be submitted to the President of the Office for Personal Data Protection in an electronic form only, i.e., using a qualified electronic signature (QES) or ePUAP trusted profile, which is a Polish nationwide platform for communication of citizens with public administrations in a uniform and standardized way. Apart from notification to the President of the Office for Personal Data Protection, the PDPA requires the entity appointing the DPO to publish the contact details of the appointed DPO on its website or — if it does not have a website — in another generally applicable manner. Polish data protection authority has explained that those data should be published in an easily accessible place on a webpage (e.g., in a "Contact tab" or subpage) and has considered it inappropriate to provide the DPO's contact details in a privacy notice published on a website.
Portugal	N/A — no adopted National Data Protection Law yet.
Romania	Link to the National Data Protection Law 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 Law is available at: https://www.dataprotection.ro/?page=Legea_nr_190_2018&lang=en High-level overview of the key provisions of the National Data Protection Law 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 apply only if the employer used other less intrusive methods which did not render appropriate results in the past 3. 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 iii. statistical and archiving purposes Details on how the National Data Protection Law made use of specific opener clauses of the GDPR 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 other than those stipulated in the GDPR related to the: 1. specific appointment procedure 2. relevant activity of the DPO 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. The Law empowers the Romanian Certification Association to set the requirements along with the Romanian Data Protection Authority ("Authority") regarding the certification providers. 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 imposed. 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. There are no specific provisions referring to article 10 GDPR. However, on a related matter, concerning the employment relationship, the Law limits the implementation of monitoring systems targeting the employees, and which can be used for internal investigations. According to the Law, monitoring employees through electronic means at the workplace (in order to achieve the legitimate interests pursued by the employer) is only permitted when: 1. the legitimate interests pursued by the employer are strongly justified and prevail over the interests or rights and freedoms of the data subject 2. the employer has distributed a prior, mandatory, complete and explicit information of the employees 3. the employer has consulted the trade union or, as the case may be, the representatives of the employees before implementing the monitoring systems 4. other less intrusive forms and ways to achieve the purpose pursued by the employer have not previously proved their effectiveness 5. the retention period of personal data is proportional to the processing purpose, but not more than 30 days, except for cases expressly regulated by law or in duly justified cases According to the Law, the processing of a national ID number, including also the collection or disclosure of documentation which contains the national ID number, processed on the ground provided by art. 6, par. (1), lit. (f) of GDPR, shall be carried out by the data controller only if such controller has implemented the following specific safeguards: 1. implementation of appropriate technical and organizational measures, especially the principle of data minimization and ensuring the security and confidentiality of the personal data processing, in accordance with the provisions of Art. 32 of GDPR 2. appointing a Data Protection Officer 3. setting the retention time-limits according to the nature of the data and the purpose of their processing, as well as specific time-limits within which the personal data must be deleted or revised with a view to the deletion thereof 4. regular training regarding the obligations of the individuals who, under the direct authority of the data controller or data processor, process personal data
Slovakia	Link to the National Data Protection Law 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 is available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/ High-level overview of the key provisions of the National Data Protection Law 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. 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

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. 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.

3. 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.

4. Limitation of data controllers' obligations as set out in Articles 12 to 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. to v.

   vii. protection of the independence of the judiciary system and of judicial proceedings

   viii. protection of a data subject or rights and freedoms of others

   ix. enforcement of legal claims

   x. economic mobilization

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

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 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 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. **1. Article 8 GDPR (age for minor consent)** The new act mirrors the Article 8 GDPR and there are no specific local law requirements concerning this matter. **2. Article 10 GDPR (processing of data relating to criminal convictions and offenses especially in the employment relationship, e.g., background checks, whistleblowing hotlines, internal investigations)** Under the new act, the processing of personal data related to criminal convictions and offenses is only permissible on the basis of specific regulation or international treaty by which the Slovak Republic is bound. As regards employment relationship, under Section 41(6) of Slovak Act No. 311/2001 Coll., Labour Code, as amended, an employer may not request from a natural person information on clean criminal record, except for work where clean criminal record is required under the special regulation, or if clean criminal record is demanded by the nature of work which the natural person is to perform. Under the Slovak statutory regulation, the clean criminal record is required from employees such as state officials, police officers or firemen, legal counsels, notaries, tax advisors, etc. **3. Article 23 GDPR** The new act essentially mirrors the Article 23 GDPR, with the addition of *economic mobilization* as the legitimate grounds for restriction of data subject rights. **4. Article 37(4) GDPR (additional thresholds requiring the appointment of a DPO)** The new act does not set forth any additional thresholds for the appointment of a DPO. **5. Article 49 (5) GDPR (restrictions on the transfer of sensitive data to third countries without an adequacy decision)** The new act does not provide for any restrictions on the transfers of sensitive data to third countries. **6. Article 87 GDPR (specific rules for the processing of national IDs)** The new act expressly allows the processing of personal identification numbers only when it is necessary for the purpose of processing. It also prohibits publication of the personal identification number, unless such publication is carried out by the data subject itself. 7. No filing and/or notification obligations with the national data protection authority are provided by the new act.
Slovenia	N/A — no adopted National Data Protection Law yet.
Spain	Link to the National Data Protection Law The Spanish Parliament recently approved the statute completing the local implementation of the GDPR: the Personal Data Protection Act ("PDPA"). It was published in the Spanish Official Gazette on 6 December 2018 and is applicable as of 7 December. The new regulation is available (in Spanish only) at: https://www.boe.es/buscar/act.php?id=BOE-A-2018-16673

High-level overview of the key provisions of the National Data Protection Law

The PDPA sets forth new rules over the processing of personal data to fully implement the GDPR in Spain. Apart from specifying certain points of the GDPR that required national development, the PDPA also introduces certain novelties:

1. The PDPA establishes that the explicit consent of data subjects is not enough to allow the processing of certain special categories of personal data: Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or sexual orientation.
2. Articles 19-27 of the PDPA foresee specific types of processing that are either considered or presumed lawful by law, although they are subject to specific requirements. Said types or processing include: The data processing of contact details for professional communications and individual entrepreneurs' data, credit information systems, processing of data for video-surveillance purposes, processing of data for the inclusion of data subjects in lists to avoid commercial communications (Robinson lists), or whistleblowing.
3. The representative is considered jointly liable with the non-EU data controller or processor for non-compliance with the GDPR.
4. The Act enlarges and details cases in which a DPO must be appointed according to the GDPR.
5. The Act complements the sanctions system set forth by the GDPR and adapts to the Spanish legal system. The Act defines the traditional distinction between minor, serious and very serious infringements. Regarding the amount of the sanctions, the Act expressly refers to the GDPR. The statutes of limitation for the sanctions depend on the severity of the infringement.
6. The Act introduces a new Section regarding individuals' rights in the online environment that, in some cases, overlaps with rights and obligations laid down in the GDPR, such as:
    i. the rights to net neutrality, universal access to the internet, digital security and digital education
    ii. the right against social networks to rectify content that may infringe other rights of the user
    iii. the right to update information in digital media
    iv. digital rights in the labor context (for instance: right to digital disconnection, right to use of video-surveillance and audio-recording devices in the workplace, and the right to privacy related to the use of geolocation systems in the context of employment)
    v. the right to be forgotten in online researches
    vi. the right to be forgotten and the right to portability in social networks and equivalent services
    vii. the right to a digital will

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

1. The Spanish Personal Data Protection Act ("PDPA") develops the competence conferred by Article 8.1 GDPR, establishing that minors aged 14 and above will be allowed to provide consent for the processing of their personal data. This therefore does not change with respect to previous Spanish data protection legislation.
2. As stated by Article 10 in fine of the GDPR, the PDPA entrusts the processing of a comprehensive register of criminal convictions and offenses to the "System of assistance registers of the Justice Administration". This system includes several official registers such as the Central Register of Criminal Offenders, the Central Register for the Protection of Victims of Domestic Violence and Gender-based Violence and the Central Register of Sexual Offenders, among others. Other processing of personal data relating

	criminal convictions and offenses must be allowed by law, either by a national law or by European Union law. The PDPA specifically allows the processing of this type of data by lawyers and solicitors in the performance of their duties. 3. Article 12 of the PDPA foresees the possibility of specific regulation to affect the rights of the data subject described in Chapter III of the GDPR (Rights of the data subject, Articles 12 to 23). In such case, specific provisions shall prevail over the PDPA. 4. The PDPA sets forth a list of specific entities in which it is mandatory to appoint a DPO. Thus, among others, it is noteworthy to highlight the obligation to appoint a DPO for: Professional bodies, entities operating and providing electronic communications networks and services, information society services providers that perform profiling on a large scale, financial institutions, companies that develop advertising activities, insurance and reinsurance companies, companies providing investment services, or health centers obliged to keep clinical records. The appointment or the cessation of the DPO (either voluntary or mandatory) must be communicated to the supervisory authority within a term of 10 working days. 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. 5. Regarding the processing of national IDs, the PDPA sets forth specific rules only for those cases in which the data controller is a public body. Particularly, the public body must avoid making available to the public administrative acts that contain both the name and surname of the data subject and its national identification number (or passport number). The previous obligation to communicate the files of personal data being processed by the data controller to the Spanish Data Protection Agency was abolished with the coming into force of the GDPR. Apart from the notification obligations established in the GDPR, the PDPA sets forth the obligation to notify the creation of commercial communications opt-out lists (Robinson lists). Additionally, data controllers willing to conduct commercial communications must previously consult the lists of this nature made available to the public by the competent data protection authority and exclude the data subjects contained in it.
Sweden	Link to the National Data Protection Law 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. The NDPL is available at: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2018218-med-kompletterande-bestammelser_sfs-2018-218 High-level overview of the key provisions of the National Data Protection Law Some notable provisions of the NDPL are: **1. 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 statistic activities. Sensitive personal data may be processed under Article 9 seg. 2 (h) 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. to vi. above is allowed provided that the duty of confidentiality required under Article 9.3 GDPR is fulfilled. **2. 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. **3. "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. **4. 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). Details on how the National Data Protection Law made use of specific opener clauses of the GDPR **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. 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, ordinance, regulation or administrative order that permits organizations other than the authorities to process such data in certain cases. **3. 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.
UK	Link to the National Data Protection Law 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: 1. repeals and replaces the UK Data Protection Act 1998 2. supplements the GDPR by including certain derogations and options from the GDPR which are left to the authority of individual EU Member States 3. 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)

4. implements the EU Law Enforcement Directive (regarding data processing for criminal law enforcement purposes)
5. establishes data protection standards for data processing by intelligence services for national security purposes
6. is available at:

   http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

By means of the European Union (Withdrawal) Act 2018 which was adopted on 26 June 2018, the GDPR together with the DPA will be retained as UK data protection legislation after the UK leaves the EU.

High-level overview of the key provisions of the National Data Protection Law

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 safeguards for automated decision-making, such as profiling, which were required in the Data Protection Act 1998 have been carried over to the DPA.
4. Conditions for processing data for research, statistics or archiving purposes are similar to those set out in the Data Protection Act 1998.
5. 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.
6. 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.
7. 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
   ii. altering data to prevent its disclosure following a data subject access request
8. The Secretary of State may make future regulations to require data controllers to:
   i. pay a charge to the ICO
   ii. provide information to the ICO for the determination and collection of the charge, which will continue to fund the ICO's activities

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

1. Age of minors (Art. 8 GDPR)

The minimum age for minors to consent to data processing in relation to information society services is set at 13.

2. Data protection officer

The DPA does not provide for additional circumstances requiring organizations to appoint a DPO (additional to the circumstances set out under the GDPR).

3. **Processing of data relating to criminal convictions and offenses (Art. 10 GDPR)**

   Under the DPA, the processing of personal data relating to criminal convictions and offenses is permitted if it satisfies one of the conditions in Schedule 1 to the DPA. This includes, among others, conditions relating to employment, health, substantial public interest and consent.

   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 under Article 5 of the GDPR and rules for data retention and deletion in relation to such data.

   When relying on certain conditions for processing under Schedule 1 of the DPA, the data controller's record of processing under Article 30 of the GDPR must also include:

   i. which condition is relied on

   ii. how the processing satisfies Article 6 of the GDPR

   iii. whether the personal data is retained and erased in accordance with the appropriate policy document, and if it is not, the reasons for not following those policies

4. **Data subject rights**

   The exceptions regarding data subject rights set out in the Data Protection Act 1998 are largely replicated in the DPA. These are set out in Schedule 2 to the DPA, and exempt data controllers from certain obligations in relation to data subject rights which apply in the context of, among others, crime, taxation, immigration and journalism.

5. **Restrictions on the transfer of sensitive data to third countries without an adequacy decision (Art. 49 (5) GDPR)**

   The DPA does not set out any specific further restrictions on the transfer of sensitive data to third countries without an adequacy decision under Article 49(5) GDPR.

6. **Specific rules for the processing of national IDs (Art 87 GDPR)**

   The DPA does not set out specific rules for the processing of a national identification number in the UK.

7. **Any requirements for filings and/or notifications with the national data protection authority**

   The UK data protection authority requires payment of a "Data Protection Fee" by organizations and sole traders, unless they are exempt. There are three levels of fee corresponding to the organization's size:

   i. micro-organizations (maximum turnover of GBP 632,000 for the financial year or no more than 10 members of staff): GBP 40

   ii. small and medium-sized organizations (maximum turnover of GBP 36 million for the financial year or no more than 250 members of staff): GBP 60

   iii. large organizations (organizations that exceed the turnover or staff figures stated in Tier 1 and Tier 2): GBP 2,900

   The grounds for exemption are quite complex and limited and generally only apply if the entity is processing data relating to its own internal business operations, if it is, for example, processing personal data only for one (or more) of the following purposes:

   i. staff administration

   ii. advertising, marketing and public relations

   iii. accounts and records

   iv. not-for-profit purposes

	v. personal, family or household affairs vi. maintaining a public register vii. judicial functions viii. processing personal information without an automated system such as a computer ix. as this is just a summary, legal advice is best obtained on whether an exemption is available

Question 2 — Draft Bills for National Data Protection Laws

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. a link to such draft bill if available
b. a high-level overview of the key provisions and when such draft bill is expected to be adopted
c. if available, any details on how the draft bill makes use of specific opener clauses of the GDPR, in particular:
   i. Article 8 GDPR (age for minor consent)
   ii. Article 10 GDPR (processing of data relating to criminal convictions and offenses especially in the employment relationship, e.g., background checks, whistleblowing hotlines, internal investigations)
   iii. Article 23 GDPR (relevant restrictions on data subject rights)
   iv. Article 37(4) GDPR (additional thresholds requiring the appointment of a DPO)
   v. Article 49(5) GDPR (restrictions on the transfer of sensitive data to third countries without an adequacy decision)
   vi. Article 87 GDPR (specific rules for the processing of national IDs)
   vii. any requ**irements for filings and/or notifications with the national data protection authority**

Austria	N/A — see response to Question 1
Belgium	N/A — see response to Question 1
Bulgaria	Link to the Draft Bill 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: https://www.parliament.bg/bg/bills/ID/78179 High-level overview of the key provisions of the National Data Protection Law 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. A bill amending the existing Law on Personal Data Protection was only approved at first hearing by the Bulgarian Parliament on 19 September 2018. In order to become a good law, those amendments must be approved at a second hearing by the Bulgarian Parliament. Although the term for proposals for amendments before the second reading and voting expired on 3 October 2018, the draft bill has not been approved as of 10 December 2018. Therefore, the draft bill is subject to possible amendments and its wording should be deemed neither final nor binding at this stage. Details on how the National Data Protection Law made use of specific opener clauses of the GDPR **1. Age of minors (Art. 8 GDPR)** The age of consent under the draft bill is lower than the age under Art. 7 GDPR, and namely — 14 years. **2. Processing of data relating to criminal convictions and offenses (Art. 10 GDPR)**

	The draft bill contains no specific provisions in light of Art. 10 GDPR. In terms of employment relationship: An employer may require criminal record certificates only if the employer is expressly authorized to do so under the law. Although the consent of an employee used to be a valid legal ground for processing criminal record data for employment purposes, following the effective date of the GDPR, the consent of the employee no longer provides justification for lawful processing of criminal offenses data. Therefore, criminal record checks are generally prohibited and only possible if expressly authorized by Bulgarian law. **3. Data subject rights** Restrictions on the data subject rights under the GDPR are replicated in the draft bill. The terms and conditions for application of the restrictions is subject to separate legislation. **4. Data protection officer** The draft bill does not provide for additional circumstances requiring organizations to appoint a DPO (additional to the circumstances set out under the GDPR). **5. Restrictions on the transfer of sensitive data to third countries without an adequacy decision (Art. 49 (5) GDPR)** There are no general restrictions in the draft bill. **6. Specific rules for the processing of national IDs (Art 87 GDPR)** The draft bill imposes restrictions relating to copies of ID cards, driving licenses and passports. The data controller could make copies of these documents only in case required by law. **7. Any requirements for filings and/or notifications with the national data protection authority** There are no filing and/or notifications with the national data protection authority beyond those in the GDPR.
Croatia	N/A — see response to Question 1
Czech Republic	Link to the Draft Bill The draft of the new act on data processing is currently publicly available at the following link, together with amending legislation: https://apps.odok.cz/attachment/-/down/KORNAX99Z8Z1 Please note that since the proposed draft act has not yet been approved by the Czech legislative bodies, it is subject to possible amendments and its wording should be deemed neither final nor binding at this stage. High-level overview of the key provisions of the National Data Protection Law 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 has just passed the third reading in the chamber of deputies and should soon advance to the Senate (second chamber of the Parliament of the Czech Republic). Afterwards, the Senate has a constitutional period

of 30 days to decide on the bill. Due to the fact that Senate may still reject the bill, the exact (or even estimated) date of enactment of the new act remains unknown.

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 to 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
    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.

Details on how the National Data Protection Law made use of specific opener clauses of the GDPR

1. **Article 8 GDPR (age for minor consent):**

    Under the draft act, the age limit for a child to grant consent to the offer of information society services is reduced to 15 years of age. Therefore, the processing of the personal data of a child would be lawful where the child is at least 15 years old, otherwise the consent given or authorized by the holder of parental responsibility over the child would be necessary.

2. **Article 10 GDPR (processing of data relating to criminal convictions and offenses especially in the employment relationship):**

    Under the draft act, the processing of personal data related to criminal convictions and offenses is permissible when used adequately for journalistic, academic, artistic or literary purposes if such processing is necessary to achieve a legitimate objective, in particular on matters of public interest, and if the legitimate interest in the processing of such personal data prevails over the legitimate interests of the

	data subject. As regards employment relationship, under section 316(4) of Czech Act No. 262/2006 Coll., Labour Code, as amended, an employer may not require from an employee proof of clean criminal record, unless there is a cause for such requirement consisting in the nature of work to be performed, provided that the requirement is adequate, or in the cases where such requirement is stipulated by the special regulation. Under the Czech statutory regulation, a clean criminal record is required from employees such as state officials, police officers or firemen, legal counsels, notaries, tax advisors, etc. **3. Article 23 GDPR (relevant restrictions on data subject rights):** Under the draft act, data subject right to access pursuant to Article 15 GDPR may be restricted, suspended or not applied at all if necessary and appropriate for the purposes of protection of rights or legitimate interests of other persons. **4. Article 37(4) GDPR (additional thresholds requiring the appointment of a DPO):** No additional thresholds requiring the appointment of a DPO are set forth by the draft act. **5. Article 49 (5) GDPR (restrictions on the transfer of sensitive data to third countries without an adequacy decision):** No restrictions on the transfers of sensitive data to third countries is provided by the draft act. **6. Article 87 GDPR (specific rules for the processing of national IDs):** No specific rules for the processing of national IDs are provided by the draft act. 7. No filing and/or notification obligations with the national data protection authority are provided by the draft act.
Cyprus	N/A — see response to Question 1
Denmark	N/A — see response to Question 1
Estonia	N/A — see response to Question 1
Finland	N/A — see response to Question 1
France	N/A — see response to Question 1
Germany	N/A — see response to Question 1
Greece	Link to the Draft Bill 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. The Draft Bill is available in Greek at: http://www.opengov.gr/ministryofjustice/wp-content/uploads/downloads/2018/02/sxedio_nomou_prostasia_pd.pdf High-level overview of the key provisions of the Act on Introducing the PDPA Noteworthy provisions of the draft bill include the following:

	1. Provisions are introduced for CCTV data processing. 2. 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: i. evaluating an employee's suitability for work ii. compliance with a legal obligation iii. establishing 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) 3. Provisions are introduced regarding processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. 4. Criminal sanctions are being introduced for breach of the GDPR provisions including imprisonment for up to five years and a fine of up to EUR 300,000. Stricter sanctions are envisaged if breach has an impact on national security. 5. A DPO who violates his/her duty of confidentiality (as envisaged by the draft bill) can be sanctioned with imprisonment for up to five years and a fine of up to EUR 100,000. Details on how the Act on Introducing the PDPA made use of specific opener clauses of the GDPR 1. The minor age for consent is set at 15 years. 2. Processing of data relating to criminal convictions and offenses is permissible when provided by law which sets the purpose, safeguards and measures for the protection of the data subject rights. As a matter of exception, such processing is also permissible (*inter alia*) in the context of employment if absolutely necessary for evaluation of suitability for a specific position (relevant information can be obtained by the employee directly from the employer or from a third party on the basis of the employee's prior written consent). 3. The controller can (partially of fully) refuse a data subject right if processing is related to i. national security ii. defense iii. public security iv. the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security v. important economic or financial interest of the Greek state vi. the establishment, exercise or enforcement of law claims vii. the protection of the data subject or the rights and freedoms of others 4. Further to the GDPR provisions, appointment of a DPO is required for controllers and processors whose processing operations, according to the authority's relevant issued categories, require regular and systematic monitoring of data subjects on a large scale by virtue of their nature, their scope and/or their purposes. 5. There is no requirement to register databases that contain personal data or to register as a processor of personal data. Only requirement is to notify the appointment of a DPO with the Greek Data Protection Authority.
Hungary	N/A — see response to Question 1

Ireland	N/A — see response to Question 1
Italy	N/A — see response to Question 1
Latvia	N/A — see response to Question 1
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 1
Portugal	Link to the Draft Bill The Council of Ministers recently approved Draft Bill No. 120/XIII that will ensure the implementation of the GDPR in Portugal — available here: https://www.cnpd.pt/bin/decisoes/Par/ppl120-XIII.htm High-level overview of the key provisions of the Draft Bill The draft bill is still subject to changes as it will have to be approved by parliament. The first discussion of the draft bill in parliament was held on 3 May 2018, where it was heavily criticized by several political parties and by the national Commission for Data Protection (*Comissão Nacional de Proteção de Dados* (CNPD). It is now being studied by a special group of the Portuguese Parliament, so Portugal is currently subject to the Law 67/98 of 26 October (Personal Data), enacted 26 October 1998. 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 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. 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. 7. 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. 8. 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

ii. the period that is necessary for the purpose of the processing. However, it also adds that:

iii. where, by the nature and purpose of the processing, it is not possible to establish the data retention period, the retention of the data shall be deemed lawful

iv. 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.

9. 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:

   i. 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)

   ii. the processing of biometric data of employees (only allowed for the control of attendance and control of access to the premises)

   iii. 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)

10. With regards to public entities, the draft bill contains detailed indications on the possible options for appointment of a single DPO for different entities.

11. 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.

12. The draft bill also contains specific provisions concerning the processing of data in the context of:

   i. public procurement proceedings

   ii. health databases or centralized registers

   iii. archiving purposes in the public interest

   iv. 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

13. 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.

14. 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):

   i. very serious administrative offense (with a statute of limitation period of three years)

	ii. serious administrative offense (with a statute of limitation period of two years) iii. minor administrative offense (with a statute of limitation period of one year) 15. 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. Details on how the Draft Bill made use of specific opener clauses of the GDPR **1. Age of minors (Art. 8 GDPR)** 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. **2. Processing of data relating to criminal convictions and offenses (Art. 10 GDPR)** The draft bill foresees a list of criminal offenses similar to that which was already included in the previously existing Portuguese Data Protection Law. **3. Data subject rights** 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. **4. Data protection officer** In this respect, the Portuguese Bar Association has reacted to the development of law practice and DPO functions at the same time. In its Opinion 14/PP/2018-G, the Portuguese Bar Association considered that, according to their professional statutes, combining these two roles is forbidden. Another particularity regarding this matter is expressly indicated in the online form made available by the CNPD for the designation of the DPO, which states that "The DPO must be a natural person (even if you belong to a company that provides DPO services)". With regards to public entities, the draft bill contains detailed indications on the possible options for appointment of a single DPO for different entities. **5. Any requirements for filings and/or notifications with the national data protection authority** The CNPD has approved Regulation no. 1/2018 (published in the Official Gazette as Regulation nr. 798/2018, of 30 November), pursuant to Articles 35, (4) and 57 (1) (k) of the GDPR, which provides a list of personal data processing activities that must be subject to a Data Protection Impact Assessment. Through this Regulation, the CNPD clarifies which situations, in addition to those already foreseen in Article 35 (3) of the GDPR, in which, prior to the processing of personal data, the Controller shall carry out a DPIA.
Romania	N/A — see response to Question 1
Slovakia	N/A — see response to Question 1
Slovenia	In Slovenia, the new Data Protection Act has not yet been adopted. The task of the preparation of the act has been given to the Ministry of Justice, which submitted a draft act to the parliament in April 2018. However, during the procedure before the parliament, the mandate of the previous parliament ended and therefore the legislative procedure for the act was terminated. Following these developments, the Ministry of Justice is in process of preparing a new draft Data Protection Act, which has not yet been made available to the public. Accordingly, the contents of the new

	act are not yet known.
Spain	N/A — see response to Question 1
Sweden	N/A — see response to Question 1
UK	N/A — see response to Question 1

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.