



## AUSTRIA

## GDPR Implementation Tracker



## NAME

Bundesgesetz,  
mit dem das  
Datenschutzgesetz  
2000 geändert  
wird (Datenschutz-  
Anpassungsgesetz  
2018)

STATUS: ADOPTED

## LAWFULNESS OF PROCESSING (ART 6)



No Deviations

## CHILD'S CONSENT (ART 8)



**ADDITIONAL REQUIREMENT:** For information society services offered directly to children, consent within the meaning of Art 6(1)(a) GDPR is valid if the child has reached 14 years of age (§ 4(4) DSG 2018).

## SENSITIVE DATA (GENETIC, BIOMETRIC AND HEALTH DATA) (ART 9(4))



No Deviations

## CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)



**SPECIFYING PROVISIONS:** Processing of personal data relating to acts or omissions that are punishable under criminal or administrative provisions—especially regarding the suspicion of commission of a crime—as well as data relating to criminal convictions or preventive measures is permitted if:

1. An express statutory authorization or duty to process such data exists.
2. The permissibility of processing such data otherwise results from statutory duties of care or is necessary to pursue the legitimate interests of the controller of a third party under Art 6(1)(f) GDPR—and the manner in which such data are processed protects the interests of the data subject according to the GDPR. (See § 4(3) DSG 2018).

## AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)



No Deviations

## RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

**RESTRICTING PROVISIONS:**

**1. Right of Correction** (Art. 16 GDPR): If the correction of data processed in an automated manner cannot occur immediately because—for technical or economic reasons—correction can only occur at a particular point in time, processing of the data must be restricted under Art 18(2) GDPR until they can be corrected (§ 4(2) DSG 2018).

**2. Right of Erasure** (Art. 17 GDPR): If the deletion of data processed in an automated manner cannot occur immediately because—for technical or economic reasons—deletion can only occur at a particular point in time, processing of the data must be restricted under Art 18(2) GDPR until they can be deleted (§ 4(2) DSG 2018).

## JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))



No Deviations

## AD HOC NOTIFICATIONS - RECORDS OF PROCESSING ACTIVITIES (ART 30)

**ADDITIONAL PROVISIONS:**

**1. Ad hoc authorization request for scientific or statistical processing:** If no statutory grounds supporting scientific research or statistical processing are present, controllers must apply to the Austrian DPA for authorization. (§ 7(3) DSG 2018).

**2. Authorization request for transfers of address data:** If statutory grounds supporting the “transfer of the address data of a large group of persons” are not present, the controller wishing to conduct the transfer must apply to the Austria DPA for authorization. (§ 8(3) DSG 2018).

## SECURITY OF PROCESSING (ART 32)

**ADDITIONAL PROVISIONS:**

In the CCTV monitoring context:

**(a)** Controllers must implement “suitable information security measures” that are tailored to the risk and must ensure that no unauthorized access to CCTV recordings and unauthorized alteration of CCTV recordings occur.

**(b)** When not using CCTV for live real-time monitoring, controllers must log every processing performed on CCTV data.

**(c)** Recordings must be deleted within 72 hours, unless the controller can document and justify a longer retention period.

(See § 13 DSG 2018).

## AUSTRIA

## DATA BREACH (ART 33 &amp; 34)



No Deviations

## DATA PROTECTION OFFICER (ART 37(4))

**ADDITIONAL PROVISIONS:**

**1. Duty of Confidentiality:** DPOs and all persons working for them are bound to maintain confidentiality regarding the fulfillment of their tasks. This duty exists in addition to any other duties of confidentiality they may be subject to, and survives the termination of the DPO's service as DPO.

**2. Evidentiary Privilege:** If the DPO learns of any matter that is subject to a statutory evidentiary privilege, the privilege can also be exercised by the DPO and his/her staff to the extent that the privilege holder has elected to exercise it.  
(See § 5(1), (2) DSG 2018).

## DATA TRANSFER DEROGATIONS (ART 49(5))



No Deviations

POWERS SUPERVISORY AUTHORITIES  
(ART 58)**SPECIFYING PROVISIONS:**

The Austrian DPA is expressly authorized to:

- (a) Request information, require production of documents, and require descriptions of data processing.
- (b) Conduct on-site inspections, operate data processing systems, and make copies of data storage media.
- (c) Impose interim emergency measures to protect duties or obligations of confidentiality, such as suspending processing in whole or in part.
- (d) Impose monetary fines on natural and legal persons.  
(See § 22 DSG 2018).

Decisions by the Austrian DPA may be appealed to the Austrian Supreme Federal Administrative Court (*Bundesverwaltungsgericht*) (§ 27 DSG 2018).

## CLASS ACTIONS (ART 80 (2))



Nonprofit organizations active in the field of data protection may represent individual consumers in:

- (a) Proceedings before the Austrian DPA.
- (b) Challenges of Austrian DPA rulings before the Austrian administrative courts.
- (c) Civil suits against data controllers in the Austrian civil courts, including suits for damages.  
(See § 28 DSG 2018).

Suits for damages are subject to "the general provisions of civil law" (§ 29 DSG 2018).

## ADMINISTRATIVE SANCTIONS (ART 83)

**RESTRICTING PROVISIONS:**

1. The Austrian DPA can impose monetary sanctions against legal persons if a violation of the GDPR and either § 1 DSG 2018 or Chapter 1 DSG 2018 has occurred, and either:
  - (a) The violation was committed by a person who had a "leadership position" in the legal person; or
  - (b) The violation was made possible by negligent supervision of other employees by a person in a "leadership position."

2. No fines are permitted against governmental entities or other public controllers.

(See § 30 DSG 2018).

## PENALTIES (ART 84)



No Deviations

## HR PROCESSING (ART 88)

**SPECIFYING PROVISIONS:**

The Austrian GDPR implementation statute states that the Austrian Works Constitution Act (*Arbeitsverfassungsgesetz*) constitutes a law implementing Art 88 GDPR, to the extent that it regulates the processing of personal data (§ 11 DSG 2018).

## HR PROCESSING (ART 88)

**SPECIFYING PROVISIONS:**

**1. Conditions for Scientific Research or Statistical Processing:** Personal data may be processed for scientific research or statistical purposes if:

- (a) It is publicly accessible;
- (b) The controller obtained the data through other investigations or for other purposes via permissible means; or
- (c) The data are pseudonymized for the controller and it cannot identify the data subjects via legally permitted means.

Personal data that do not fall into the above categories may only be processed for scientific research or statistical purposes:

- (a) In accordance with specific statutory provisions;
- (b) With the consent of the data subject(s); or
- (c) With the authorization of the Austrian DPA.

**2. Anonymization Requirement:** Personal data must be anonymized as soon as the scientific research or statistical purposes no longer require identifiable data.

(See § 7 DSG 2018).

## OBLIGATIONS OF SECRECY (ART 90)

**SPECIFYING PROVISIONS:**

Austria maintains the doctrine of "data secrecy": In addition to any other obligations of secrecy/confidentiality imposed by law, controllers, processors, and their personnel must keep confidential all personal data that they obtain during their professional activity, except to the extent that the law permits the disclosure and/or transfer of such data. (See § 6 DSG 2018).

## LOCAL DPA GUIDANCE &amp; LEGAL SOURCES



[Data Protection Amendment Act 2018](#)



## BELGIUM

### NAME

Wet tot Oprichting van de Gegevensbeschermingsautoriteit

STATUS: ADOPTED

### LAWFULNESS OF PROCESSING (ART 6)

✗  
No Deviations

### CHILD'S CONSENT (ART 8)

✗  
No Deviations

### SENSITIVE DATA (GENETIC, BIOMETRIC AND HEALTH DATA) (ART 9(4))

✗  
No Deviations

### CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

✗  
No Deviations

### AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

✗  
No Deviations

### RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

✗  
No Deviations

### JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

✗  
No Deviations

### AD HOC NOTIFICATIONS - RECORDS OF PROCESSING ACTIVITIES (ART 30)

✗  
No Deviations

### SECURITY OF PROCESSING (ART 32)

✗  
No Deviations

### DATA BREACH (ART 33 & 34)

✗  
No Deviations

### DATA PROTECTION OFFICER (ART 37(4))

✗  
No Deviations

### DATA TRANSFER DEROGATIONS (ART 49(5))

✗  
No Deviations

### POWERS SUPERVISORY AUTHORITIES (ART 58)



#### ADDITIONAL/VARYING REQUIREMENT:

The DPA is granted investigative, corrective, and advisory powers, as provided in the GDPR, but the Belgian Act provides for specifications compared to the GDPR leading to more far-reaching powers of the DPA. Therefore, the

DPA's investigative powers amount to the following additional powers: (1) written and oral interrogations; (2) consulting IT systems and copying all data on these systems; (3) consulting information electronically; (4) seizing or sealing IT systems or goods; and (5) claiming the identification of a subscriber or usual user of an electronic communications service or of the used means of electronic communications (Art 66 Belgian Act) (Art 58(1) GDPR).

Against certain preliminary measures taken by the DPA, the defendant may file a (non-suspensive) appeal (Art 70–71 Belgian Act and Art 58(2) GDPR). The defendant may also file an appeal against acts of seizure and sealing, as described above (Art 90 Belgian Act and Art 58(1) GDPR). In the same way, the DPA's corrective powers are also broadened so that they also explicitly include: (1) proposing settlements to the parties involved; (2) dismissing a complaint; (3) transferring the case to the public prosecutor to decide on criminal prosecution; (4) ordering to refrain from further prosecution; (5) ordering a suspension of judgment; and (6) publishing its decision on its own website.

In terms of procedure, the DPA shall be instituted by means of six independent organs (supplemented further by independent experts and a reflection council): an executive committee, general secretariat, frontline service, knowledge center, inspection body, and dispute resolution chamber. Procedurally, parties are granted the option, before the DPA's dispute resolution chamber, to submit any evidence or defense elements and to request to be heard. Involved parties can file an appeal against the decision of the disputes resolution chamber with the Commercial Court of Appeal (*Marktenhof*, a court competent to treat appeals also against decisions taken by the Belgian Competition Authority, Financial Services and Markets Authority, Belgian Institute for Postal Services and Telecommunications, and other comparable administrative authorities).

#### CLASS ACTIONS (ART 80 (2))



#### SPECIFYING REQUIREMENT:

Organizations or associations may, independently of an individual's mandate, file a

**BELGIUM**

complaint with the Belgian DPA (Explanatory Memorandum, p. 40 and Art 58 of the Belgian Act) (Art 80(2) GDPR).

**ADMINISTRATIVE SANCTIONS (ART 83)****SPECIFYING/VARYING REQUIREMENT:**

The Belgian Act provides for the procedural side of imposing administrative sanctions, such as the payment term, and the content requirements of the decision to impose an administrative sanction. The Act foresees an appeal option against the decision with the Belgian Commercial Court of Appeal (Art 102 Belgian Act) (Art 83 GDPR). The Act deviates from the GDPR in the maximum fine in the case of “multiple counts” (*meerdaadse samenloop*), in which case the maximum fine exists in “the highest administrative fine times two” (Art 103 Belgian Act) (Art 83 GDPR).

**PENALTIES (ART 84)**

No Deviations

**HR PROCESSING (ART 88)**

No Deviations

**PROCESSING FOR ARCHIVING, SCIENTIFIC, HISTORICAL RESEARCH OR STATISTICAL PURPOSES (ART 89)**

No Deviations

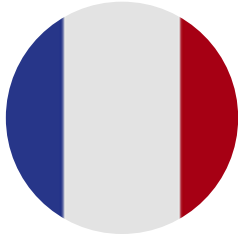
**LOCAL DPA GUIDANCE & LEGAL SOURCES**

[Wet tot Oprichting van de Gegevensbeschermingsautoriteit](#)

[Local DPA Guidance on the Belgian Act](#)

**REMARKS**

Please note that the Belgian Act merely targets the institution of the new data protection authority (previously “Privacy Commission”) and its rules of procedure. The Act does not include any other provisions that allow for national implementation under the GDPR. At this stage, we are unaware of whether Belgium will be adopting additional national legislation to reflect these other provisions.



## FRANCE

## NAME

# Project de loi relatif à la protection des données personnelles

STATUS: DRAFT

## LAWFULNESS OF PROCESSING (ART 6)



No Deviations

## CHILD'S CONSENT (ART 8)



No Deviations

SENSITIVE DATA (GENETIC, BIOMETRIC AND  
HEALTH DATA) (ART 9(4))

**ADDITIONAL/SPECIFYING REQUIREMENT:** In addition to the exceptions provided by the GDPR, certain categories of processing of health data are not subject to the requirements of the French Act: (1) processing for educational purposes; (2) processing for reimbursement purposes; (3) processing carried out by doctors within conditions in specific legislation; and (4) processing carried out by regional health agencies. Processing of health data in case of medical emergency is only to a limited extent subject to conditions in the GDPR. Notwithstanding this, the principle shall be that the CNIL adopts regulations, in cooperation with the National Institute of Health, allowing processing health data (authorizations by the French DPA are still possible but will become the exception). Processing of

health data carried out for research purposes is either legitimized upon authorization from or upon prior notification to the French DPA (Art 13 French Act) (Art 9(4) GDPR).

CRIMINAL CONVICTIONS/SECURITY  
MEASURES (ART 10)

**SPECIFYING REQUIREMENT:** Data related to criminal convictions and related security measures can only be processed by the public bodies specifically prescribed by law (Art 11 French Act) (Art 10 GDPR).

AUTOMATED INDIVIDUAL DECISION-MAKING  
(ART 22)

No Deviations

RESTRICTIONS TO DATA SUBJECT'S RIGHTS  
(ART 23)

**ADDITIONAL REQUIREMENT:** The French Act foresees that the Council of State (*Conseil d'Etat*) may lay down the processing operations and processing categories that are exempted from the individual notification obligation in case of a data breach, if such notification would lead to a national security risk or a risk to national defense or public security, and shall apply when the processing is carried out for a legitimate interest of the controller (Art 15 French Act) (Art 23 and 34 GDPR).

JOINT CONTROLLER RESPONSIBILITIES  
(ART 26 (1))

No Deviations

## GDPR Implementation Tracker

AD HOC NOTIFICATIONS - RECORDS OF  
PROCESSING ACTIVITIES (ART 30)

**SPECIFYING REQUIREMENT:** Prior notifications of data processing operations are abolished by the French Act, but it does maintain a specific formality for processing of national identification numbers (NIR). This processing operation will be governed by legislative decree, which shall determine the categories of controllers as well as the processing purposes (Art 9 French Act) (Art 30 and 6 GDPR).

## SECURITY OF PROCESSING (ART 32)



No Deviations

## DATA BREACH (ART 33 &amp; 34)



**ADDITIONAL REQUIREMENT:** The French Act foresees that the Council of State (*Conseil d'Etat*) may lay down the processing operations and processing categories that are exempted from the individual notification obligation in case of a data breach, if such notification would lead to a national security risk or a risk to national defense or public security, and shall apply when the processing is carried out for a legitimate interest of the controller (Art 15 French Act) (Art 23 and 34 GDPR).

## DATA PROTECTION OFFICER (ART 37(4))



No Deviations

## DATA TRANSFER DEROGATIONS (ART 49(5))



**ADDITIONAL REQUIREMENT:** The French DPA and Conseil d'Etat can request the European Court of Justice (ECJ) to assess the validity of an adequacy decision by the European Commission or of appropriate safeguards determined by the commission. The Conseil d'Etat may decide

## FRANCE

to suspend the data transfer based on the disputed commission decision in anticipation of the ECJ judgment (Art 17 French Act) (Art 49 GDPR).

---

**POWERS SUPERVISORY AUTHORITIES  
(ART 58)**


No Deviations

---

**CLASS ACTIONS (ART 80 (2))**


**SPECIFYING REQUIREMENT:** The French Act allows individuals to mandate an organization or association to exercise their rights with the French DPA or against the DPA in judicial court proceedings (Art 16 French Act) (Art 80(2) GDPR).

---

**ADMINISTRATIVE SANCTIONS (ART 83)**


No Deviations

---

**PENALTIES (ART 84)**


No Deviations

---

**HR PROCESSING (ART 88)**


No Deviations

---

**PROCESSING FOR ARCHIVING, SCIENTIFIC,  
HISTORICAL RESEARCH OR STATISTICAL  
PURPOSES (ART 89)**

**ADDITIONAL REQUIREMENT:**

In the case of archiving purposes in the public interest, the access, correction, restriction, portability, and objection rights of the individual shall not apply when a balancing of interests weighs in favor of the controller (Art 12 French Act) (Art 89 GDPR).

---

**OBLIGATIONS OF SECRECY (ART 90)**


No Deviations

---

**LOCAL DPA GUIDANCE & LEGAL SOURCES**


[Project de loi relatif à la protection des données personnelles](#)

[Local DPA Guidance on the French Act](#)

---

**REMARKS**

The French Act amends the current French Data Protection Act (*la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*). It does not repeal the existing Act. This is the first draft that has been published.



## GERMANY

## NAME

Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz)

STATUS: ADOPTED

## LAWFULNESS OF PROCESSING (ART 6)



## SPECIFYING PROVISIONS:

**1. Processing for New Purposes:** Non-public controllers can process personal data for purposes other than collection purposes if necessary for the establishment, exercise, or defense of civil claims (§ 24 BDSG-New).

**2. Public Controllers:** Public controllers who process data for law-enforcement purposes are subject to a separate regime for lawfulness of processing (§§ 45–85 BDSG-New).

## CHILD'S CONSENT (ART 8)



No Deviations

## GDPR Implementation Tracker

## SENSITIVE DATA (GENETIC, BIOMETRIC AND HEALTH DATA) (ART 9(4))



## ADDITIONAL/SPECIFYING PROVISIONS FOR HEALTH DATA:

**1. Processing for Medical Treatment:** Sensitive data can be processed without prior consent of the data subject so long as medical personnel—or anyone with equivalent duties of confidentiality—are responsible for the processing for these purposes: (1) preventive medicine; (2) medical diagnosis; (3) providing care or treatment in the health-care or social-services fields; (4) managing systems or services in the health-care or social-services fields; (5) determining employees' working capacity; or (6) any processing pursuant to a contract between an individual and a health professional.

**2. Health Care Company, Pharma, and Device-Related Processing:** Sensitive data can be processed without prior consent of the data subject "to ensure high standards of quality" both "within the health care industry" and "for medicinal products and medical devices."

**3. Mandatory Security Requirements:** In order to process sensitive data without consent under the above, controllers must implement statutorily enumerated information security measures.

(See § 22 BDSG-New).

For more details, see Part 2 of our five-part series, [An English-Language Primer on Germany's GDPR Implementation Statute](#).

## CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)



No Deviations

## AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)



## ADDITIONAL/SPECIFYING PROVISIONS:

**1. Automated Decisions in the Insurance**

## Context:

**(a)** Automated decisions can be used without individual consent and appeal mechanisms if the individual receives everything he or she is asking for (e.g., receives the full value of a claim).

**(b)** For health insurance, no prior consent is necessary for automated decisions based on binding fee-for-service tables for medical procedures — but the insurer must inform the individual (at the time of full or partial denial) that a human appeal mechanism is in place. (See § 37 BDSG-New).

**2. Credit Scoring:** The German statute maintains Germany's current regime for generating credit scores used in automated decisions, including: (1) only scientifically recognized statistical methods may be used to calculate scores; (2) scores cannot be based exclusively on address data, and if address data is used to calculate scores, individuals must be notified; and (3) only debts that have been the subject of a judgment, are uncontested, or are seriously delinquent can be included in credit scores. (See § 31 BDSG-New).

For more details, see Part 4 of our five-part series, [An English-Language Primer on Germany's GDPR Implementation Statute](#).

## RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)



## RESTRICTIONS ON SPECIFIED RIGHTS:

**1. Right to Information** (Arts. 13/14 GDPR):

**(a) Confidential Information:** If companies collect data from sources other than the data subject, they do not have to provide privacy notices to the extent that doing so would reveal information considered confidential under German law (§ 29 BDSG-New).

**(b) Follow-on Notices:** Companies do not have to provide follow-on notices explaining that they are processing data for a new purpose if doing so would adversely affect the company's establishment, exercise, or defense of legal claims (§ 33 BDSG-New).

## GERMANY

**2. Right of Access** (Art. 15 GDPR):

**(a) Confidential Information:** Companies do not have to provide data in response to access requests if doing so would reveal information considered confidential under German law (§ 29 BDSG-New).

**(b) Archive or Backup Data:** Companies do not have to provide data to backup or archived data (§ 34 BDSG-New).

**3. Right of Erasure** (Art. 17 GDPR): Companies have a limited exemption to individuals' deletion rights if data is stored in a non-automated medium, deletion would require disproportionate effort, and the data subject has a comparatively minimal interest in deletion (§ 35 BDSG-New).

For more details, see Part 4 of our five-part series, [An English-Language Primer on Germany's GDPR Implementation Statute](#).

---

**JOINT CONTROLLER RESPONSIBILITIES**  
(ART 26 (1))

  
No Deviations

---

**AD HOC NOTIFICATIONS - RECORDS OF PROCESSING ACTIVITIES** (ART 30)

  
No Deviations

---

**SECURITY OF PROCESSING** (ART 32)


**ADDITIONAL REQUIREMENT:** In order to process health and/or medical data without consent, controllers must implement statutorily enumerated "suitable and specific" security safeguards, including: (1) internal policies regulating secondary uses; (2) employee training; (3) appointing a data protection officer (DPO); (4) access controls; (5) logging and monitoring; (6) encryption and/or pseudonymization; (7) backups and rapid-restore procedures; and (8) periodic security self-audits. (See § 22 BDSG-New).

For more details, see Part 2 of our five-part series, [An English-Language Primer on Germany's GDPR Implementation Statute](#).

---

**DATA BREACH** (ART 33 & 34)
**EXEMPTIONS:**

**1. Confidentiality Exemption for Notifications to Individuals:** Companies do not have to provide breach notifications to individuals to

the extent that doing so would endanger confidential information. (Art 34 GDPR).

**2. Evidentiary Privilege for Breach Notifications:** Breach notifications made to DPAs (under Art 33 GDPR) or individuals (under Art 34 GDPR) cannot be used as evidence in fining procedures against the notifying organization without its consent.

For more details, see Part 4 of our five-part series, [An English-Language Primer on Germany's GDPR Implementation Statute](#).

---

**DATA PROTECTION OFFICER** (ART 37(4))

  
No Deviations

---

**DATA TRANSFER DEROGATIONS** (ART 49(5))

  
No Deviations

---

**POWERS SUPERVISORY AUTHORITIES**  
(ART 58)
**ADDITIONAL PROVISIONS:**

**1. Powers:** The federal data protection commissioner has "the powers referred to in Article 58 of [the GDPR]." (§ 15 BDSG-New).

**2. Tasks:** In addition to the tasks listed in the GDPR, the federal data protection commissioner has the following tasks:

**(a)** To "monitor and enforce the application" of the data protection law.

**(b)** To "promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data."

**(c)** To advise the German legislature, federal government, and other institutions on "legislative and administrative measures" relating to data protection.

**(d)** To "promote the awareness of controllers and processors of their obligations" under the German privacy law.

**(e)** Upon request, to "provide information to any data subject concerning the exercise of their rights under... data protection legislation," and to "cooperate with the supervisory authorities in other Member States to that end."

**(f)** To "handle complaints lodged by a data subject" and investigate the complaint.

**(g)** To "cooperate with ... and provide mutual assistance to other supervisory authorities, to ensure the consistency of application and enforcement of... data protection legislation."

**(h)** To "conduct investigations on the application of... data protection legislation."

**(i)** To "monitor relevant developments, ... in particular the development of information and communication technologies and commercial practices."

**(j)** To provide advice when law enforcement agencies request prior consultation.

**(k)** To "contribute to the activities of the European Data Protection Board."

See § 14 BDSG-New.

**3. State DPAs:** Note that the powers and tasks of the 16 state-run DPAs are set forth in each state's data protection statutes.

---

**CLASS ACTIONS** (ART 80 (2))

  
No Deviations

---

**ADMINISTRATIVE SANCTIONS** (ART 83)
**SPECIFYING PROVISIONS:**

**1. Fines:** For the assessment of fines under German law, the procedures of Germany's Regulatory Offenses Act apply. Summarized briefly, German DPAs can issue a fine notice against companies. The company can object to the fine, after which it is forwarded via the public prosecutor to the local magistrate court for review. However, if a fine is more than €100,000, the local district court reviews the fine. (See § 41 BDSG-New).

**2. Administrative Actions other than Fines:** Administrative actions other than fines (e.g., injunctions, suspensions of transfers) are governed under Germany's administrative procedure rules. These measures are appealable to German administrative courts.

**RESTRICTION PROVISIONS:**

Germany's new data protection statute states that Germany's Act on Regulatory Offenses (*Gesetz über Ordnungswidrigkeiten*) governs the imposition of fines under the GDPR. Generally speaking, under the Act, misconduct is only attributed to organizations such that it can serve as a basis for a fine against the organization if the violation of law was committed by an employee/agent within a leadership position or was committed by a subordinate who was negligently supervised by employees in leadership positions.

For more details, see Part 5 of our five-part series, [An English-Language Primer on Germany's GDPR Implementation Statute](#).



---

**GERMANY**


---

**PENALTIES (ART 84)**

**SPECIFYING PROVISIONS:**

Penalties are permitted up to the full amounts envisioned by the GDPR. For the assessment of fines under German law, the procedures of Germany's Regulatory Offenses Act apply. (See § 41 BDSG-New).

**HR PROCESSING (ART 88)**

**SPECIFYING PROVISIONS:****1. Employment Relationship as Basis for Processing:**

**(a)** Personal data of employees may be processed for employment-related purposes when necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract.


**(b)** Sensitive data may also be processed in the HR context "if it is necessary to exercise rights or comply with legal obligations derived from labour law, social security and social protection law, and there is no reason to believe that the data subject has an overriding legitimate interest in not processing the data."

**2. Works Council Agreement as Legal Basis for Processing:**

The processing of personal data, including special categories of personal data of employees for employment-related purposes, shall be permitted on the basis of collective agreements—but Works Council Agreements must satisfy Art 88(2) GDPR. (See § 26 BDSG-New).

**3. NOTE:** Numerous other provisions relating to HR privacy are set forth in other German statutes and decisions of the German labor courts.

For a detailed discussion of HR privacy rules under Germany's new data protection statute, see Part 3 of our five-part series, [An English-Language Primer on Germany's GDPR Implementation Statute](#).

**PROCESSING FOR ARCHIVING, SCIENTIFIC,  
HISTORICAL RESEARCH OR STATISTICAL  
PURPOSES (ART 89)**

**DEROGATING PROVISION:**

**1.** Sensitive data can be processed for scientific research or statistical purposes without prior consent of the data subjects if "such processing is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data subject in not processing the data." However, sensitive data "shall be rendered anonymous as soon as the research or statistical purpose allows, unless this conflicts with legitimate interests of the data subject."

**2.** Data subject rights of access, correction, restriction, and objection are restricted "to the extent that these rights are likely to render impossible or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes." (See § 27 BDSG-New).

For further details, see Part 2 of our five-part series, [An English-Language Primer on Germany's GDPR Implementation Statute](#).

**OBLIGATIONS OF SECRECY (ART 90)**

**SPECIFYING PROVISIONS:**

**1.** Secrecy obligations in German law are set forth in non-data-protection law.

**2.** German DPAs do not have power to require production or seize data subject to obligations of secrecy when held by privilege-carrying professionals listed in § 203 of the German Criminal Code. This restriction also applies to processors engaged by such privilege-carrying professionals. (See § 29(3) BDSG-New).

For a more detailed discussion of this provision and its drafting, see Part 5 of our five-part series, [An English-Language Primer on Germany's GDPR Implementation Statute](#).

**LOCAL DPA GUIDANCE & LEGAL SOURCES**


[Data Protection Amendments and Implementation Act \(German\)](#)

[Data Protection Amendments and Implementation Act \(English translation\)](#)



## IRELAND

NAME

## Data Protection Bill

STATUS: DRAFT

## LAWFULNESS OF PROCESSING (ART 6)



No Deviations

## CHILD'S CONSENT (ART 8)



No Deviations

## SENSITIVE DATA (GENETIC, BIOMETRIC AND HEALTH DATA) (ART 9(4))



**ADDITIONAL REQUIREMENT:** Sensitive data may be processed for reasons of substantial public interest, including: (1) preventive or occupational medicine; (2) assessment of working capacity of an employee; (3) medical diagnosis; (4) provision of health or social care or treatment; (5) management of health and social care systems and services; (6) public interest reasons in the area of public health; and (7) on the basis of a contract with a health professional. In addition, biometric data specifically may be processed for identification and security purposes (Art 17 and 18 Irish Act) (Art 9 GDPR).

## CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)



**ADDITIONAL REQUIREMENT:** Criminal data may be processed for one of the following purposes: (1) risk assessment or fraud prevention; (2) in the exercise of a regulatory, authorizing, or licensing function or in determining eligibility for benefits or services; (3) to protect the pub-

lic against harm arising from malpractice from a person authorized to carry out a profession or activity; (4) for the establishment, defense, or enforcement of civil law claims; (5) for the prevention, detection, or investigation of national or EU law breaches subject to civil or administrative sanctions; (6) to ensure network and IT security and prevent cyber attacks; (7) for the rehabilitation or reintegration of offenders; (8) for the right to freedom of expression and information; and (9) to protect an individual (Art 19 Irish Act) (Art 10 GDPR).

## AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)



No Deviations

## RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)



**ADDITIONAL REQUIREMENT:** An individual's rights may be restricted by regulations made by a relevant minister in order to safeguard "important objectives of general public interest," provided this is necessary and proportionate after a balancing of interests. Such objectives of general public interest include: (1) national security and defense; (2) prevention of threats to public security and safety; (3) avoiding obstructions to justice (legal proceedings and investigation); (4) preventing and investigating criminal offenses and the execution of penalties; (5) preventing and investigating breaches of ethics for regulated professions; (6) preventing and investigating civil or administrative infringements and execution of sanctions; (7) identification of assets obtained through criminal conduct; (8) regulation of asylum and immigration; (9) tax or other duty administration; (10) safeguarding economic or financial interests of the country; (11) safeguarding smooth operation of the payments industry; (12) protecting the public health and safety and protecting the public against financial loss and discrimination; (13) protecting judicial independence; (14) maintaining registers in the public interest; (15) safeguarding public health, safety, and social protection; (16) safeguarding Cabinet

confidentiality; (17) preventing serious harm to the physical or mental health of the individual; and (18) other more specific public interests specified in regulations (Art 20 Irish Act) (Art 23 GDPR).

## JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))



No Deviations

## AD HOC NOTIFICATIONS - RECORDS OF PROCESSING ACTIVITIES (ART 30)



No Deviations

## SECURITY OF PROCESSING (ART 32)



No Deviations

## DATA BREACH (ART 33 &amp; 34)



No Deviations

## DATA PROTECTION OFFICER (ART 37(4))



No Deviations

## DATA TRANSFER DEROGATIONS (ART 49(5))



**SPECIFYING REQUIREMENT:** The minister may issue regulations allowing the restriction of data transfers for important reasons of public interest wherever there is no commission adequacy decision in place (Art 22 Irish Act) (Art 49 GDPR).

## POWERS SUPERVISORY AUTHORITIES (ART 58)



**ADDITIONAL REQUIREMENT:** The DPA can appoint "authorized officers," at its own discretion, who

## GDPR Implementation Tracker



**IRELAND**

can exercise all of the powers of the DPA. When authorized, the officer can enter any premises or place (with the exception of private homes, for which a specific warrant is required) to investigate a data protection infringement and order the provision of any document or records. The officer can also order very concrete actions, such as the provision of passwords to gain access to IT systems, and may request a warrant if entry to the premises is prevented (Art 67 Irish Act) (Art 58 GDPR). A DPA commissioner or authorized person may request information by means of information notice, which may be appealed by the investigated party (Art 69 Irish Act). The DPA's corrective powers are exercised by means of an enforcement notice, which is also open to appeal (Art 70 Irish Act). For the suspension or restriction of a processing operation or data transfer, however, the DPA must apply to the High Court, which may order such measure in case of urgency (Art 72 Irish Act).

**CLASS ACTIONS (ART 80 (2))**

No Deviations

**ADMINISTRATIVE SANCTIONS (ART 83)**

No Deviations

**PENALTIES (ART 84)**

No Deviations

**HR PROCESSING (ART 88)**

No Deviations

**PROCESSING FOR ARCHIVING, SCIENTIFIC, HISTORICAL RESEARCH OR STATISTICAL PURPOSES (ART 89)**

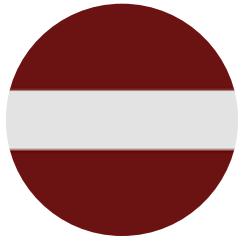
**ADDITIONAL REQUIREMENT:** The individual rights to access, correction, restriction, and objection shall not apply when processing is carried out for scientific or historical research or statistical purposes if the exercise of these rights would likely render impossible or impair the achievement of those purposes or if the controller determines such derogations are necessary for the fulfillment of those purposes. Further regulation is required to specify this (Art 25 Irish Act) (Art 23 GDPR).

**OBLIGATIONS OF SECRECY (ART 90)**

No Deviations

**LOCAL DPA GUIDANCE & LEGAL SOURCES**[Data Protection Bill](#)[Explanatory Memorandum to the Bill](#)**REMARKS**

This version of the Irish Act also contains a significant number of provisions that implement the directive. We assume the next version of the Act will include a more elaborate set of GDPR-implementing provisions.



## LATVIA

## NAME

Likumprojekts "Personas datu apstrādes likums"

STATUS: DRAFT

## LAWFULNESS OF PROCESSING (ART 6)



No Deviations

## CHILD'S CONSENT (ART 8)



**SPECIFYING REQUIREMENT:** Child's consent is lowered to the minimum of 13 years old (Art 44 Latvian Act) (Art 8 GDPR).

## SENSITIVE DATA (GENETIC, BIOMETRIC AND HEALTH DATA) (ART 9(4))



No Deviations

## CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)



**ADDITIONAL REQUIREMENT:** Criminal data may be processed upon express consent, in order to prevent an immediate significant public safety risk and in the prevention, investigation, and prosecution of crime or enforcement of criminal penalties (Art 45 Latvian Act) (Art 10 GDPR).

## AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)



No Deviations

## RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)



**SPECIFYING REQUIREMENT:** A data subject's rights may be restricted if a legitimate interest outweighs the privacy rights of the individual. A legitimate interest may exist in: (1) state security or defense; (2) protection of the democratic state and public order; (3) prevention, investigation, or prosecution of criminal or administrative infringements; (4) prevention of money laundering and terrorist financing; (5) civil liability enforcement; (6) migration policy; (7) economic and financial interests (tax, budgetary); (8) tax and fee administration; (9) public health and social protection; (10) labor relations; (11) anti-discrimination; (12) regulated professions; (13) national public registers; (14) judicial independence; (15) protection of the data subject; and (16) protection of state secrets (Art 37 Latvian Act). Despite the right of access, it is forbidden to disclose information to the individual about state institutions overseeing criminal proceedings (Art 38 Latvian Act). Data processing activities for official publication purposes are exempt from complying with individual rights requests (Art 39 Latvian Act).

## JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))



No Deviations

## AD HOC NOTIFICATIONS - RECORDS OF PROCESSING ACTIVITIES (ART 30)



No Deviations

## SECURITY OF PROCESSING (ART 32)



No Deviations

## DATA BREACH (ART 33 &amp; 34)



No Deviations

## DATA PROTECTION OFFICER (ART 37(4))



**ADDITIONAL REQUIREMENT:** The Latvian Act foresees that the Latvian DPA can provide for DPO qualification examinations (Art 6 Latvian Act) (Art 37(4) and 58 GDPR). The Latvian Act also foresees that a list must be drawn up of all DPOs nationwide, who will only qualify after passing the qualification exam organized by the Latvian DPA (Art 24–26 Latvian Act).

## DATA TRANSFER DEROGATIONS (ART 49(5))



No Deviations

## POWERS SUPERVISORY AUTHORITIES (ART 58)



**SPECIFYING REQUIREMENT:** The Latvian Act mainly foresees the same supervisory authority powers as are provided in the GDPR. It specifies slightly by including that the DPA may inspect private homes, as well as state institutions and nonresidential premises (offices) (Art 8 Latvian Act) (Art 58 GDPR).

## CLASS ACTIONS (ART 80 (2))



No Deviations



## LATVIA

---

### ADMINISTRATIVE SANCTIONS (ART 83)



No Deviations

---

### PENALTIES (ART 84)



No Deviations

---

### HR PROCESSING (ART 88)



No Deviations

---

### PROCESSING FOR ARCHIVING, SCIENTIFIC, HISTORICAL RESEARCH OR STATISTICAL PURPOSES (ART 89)



No Deviations

---

### OBLIGATIONS OF SECRECY (ART 90)



No Deviations

---

### LOCAL DPA GUIDANCE & LEGAL SOURCES



[Likumprojekts "Personas datu apstrādes likums"](#)



## THE NETHERLANDS

NAME

### Uitvoeringswet Algemene Verordening Gegevens- bescherming

STATUS: DRAFT

LAWFULNESS OF PROCESSING (ART 6)



No Deviations

CHILD'S CONSENT (ART 8)



**SPECIFYING REQUIREMENT:** When the data processing relates to an issue for which the individual is legally incapable or incompetent (when under curator or guardianship), consent must be provided by the legal representative, who can also withdraw this consent at any time (Art 5(2), (3) Dutch Act) (Art 8 GDPR).

SENSITIVE DATA (GENETIC, BIOMETRIC  
AND HEALTH DATA) (ART 9(4))



**ADDITIONAL REQUIREMENT:** The prohibition to process *genetic* data does not apply when the data were obtained directly from the data subject. In addition, the prohibition does not apply when a prevailing medical interest takes precedence or the processing is necessary for scientific research serving a public interest or for statistical purposes on the condition that the data sub-

ject explicitly gave consent (unless this is considered impossible or requires unreasonable effort) and there are specific measures to safeguard the privacy rights of the individual (Art 28 Dutch Act) (Art 9(4) GDPR).

The prohibition to process *biometric* data does not apply when it occurs for security or authentication reasons (Art 29 Dutch Act) (Art 9(4) GDPR).

An exception to the prohibition of processing *health* data for the public interest only applies when processing is carried out by specific persons (e.g., care provider, insurance companies, schools, rehabilitation institutions, a ministry in the context of a prison sentence, institutions in the context of certain social security matters) (Art 30 Dutch Act) (Art 9(4) GDPR).

CRIMINAL CONVICTIONS/SECURITY  
MEASURES (ART 10)



**ADDITIONAL REQUIREMENT:** Criminal convictions and related security measure data may only be processed in specific cases, namely when: (1) the individual provided consent; (2) it is necessary to protect vital interests of the individual or another person (in case the individual is not able to provide consent); (3) the individual made the data public; (4) the processing is necessary in light of a court case; (5) the processing is necessary for reasons of predominant public interest; (6) the processing is necessary in light of scientific research or statistical purposes; (7) processing is carried out by competent bodies appointed by criminal law or public partnerships or is necessary in light of health data processing; (8) processing is conducted upon request of the individual to take a decision about him; and (9) processing is carried out by controllers operating under a specific license. (Art 31-33 Dutch Act) (Art 10 GDPR). In case of violations of provisions (1) – (6), the authority is competent to impose the maximum fine of 4% of turnover or €20 million (Art 17 Dutch Act) (Art 83 GDPR).

## GDPR Implementation Tracker



AUTOMATED INDIVIDUAL DECISION-MAKING  
(ART 22)



**VARYING REQUIREMENT:** The prohibition included in Art 22(1) GDPR does not apply when the decision-making process based on automated decision making is necessary to comply with a legal obligation or for the performance of a task carried out in the public interest, provided the automated decision making does not include profiling. The controller shall adopt adequate means to protect the individual's privacy rights (Art 40 Dutch Act) (Art 22 GDPR).

RESTRICTIONS TO DATA SUBJECT'S RIGHTS  
(ART 23)



**SPECIFYING REQUIREMENT:** The rights of an individual younger than 16 years old or placed under curator or guardianship shall be exercised by their legal representative when the processing relates to an issue for which the individual is legally incapable or incompetent (*onbekwaam dan wel onbevoegd*) (Art 5(4) Dutch Act) (Art 23 GDPR). The rights of the individual under the GDPR can furthermore be set aside when this is necessary and proportionate in order to safeguard: (1) national security; (2) public defense; (3) public security; (4) the prevention, investigation, and prosecution of punishable acts or execution of a sentence; (5) other important interests of the Netherlands and the EU (such as monetary and economic interests); (6) the protection and independence of a judge and judicial proceedings; (7) the protection and investigation of violations of professional codes of conduct; (8) the protection of the individual or the rights and freedoms of others; and (9) the collection of requests in civil matters. These rights may also not apply to public registers in case a specific procedure for correction or completion is determined (Art 41(1) and 47 Dutch Act) (Art 23 GDPR).

## THE NETHERLANDS

JOINT CONTROLLER RESPONSIBILITIES  
(ART 26 (1))

No Deviations

AD HOC NOTIFICATIONS - RECORDS OF  
PROCESSING ACTIVITIES (ART 30)

No Deviations

## SECURITY OF PROCESSING (ART 32)



No Deviations

## DATA BREACH (ART 33 &amp; 34)



**VARYING REQUIREMENT:** Undertakings offering financial services (as defined by the Act on Financial Supervision (*Wet op Financieel Toezicht*)) are not under the obligation to notify a data breach to the individual (Art 42 Dutch Act) (Art 34 GDPR).

## DATA PROTECTION OFFICER (ART 37(4))



No Deviations

## DATA TRANSFER DEROGATIONS (ART 49(5))



No Deviations

POWERS SUPERVISORY AUTHORITIES  
(ART 58)

**ADDITIONAL REQUIREMENT:** The supervisory authority is competent to impose a "*last onder bestuursdwang*," which is remedial action (Art 16 Dutch Act) (Art 58(6) GDPR). Certain members of the Dutch supervisory authority (the members and extraordinary members of the authority, the civil servants of the secretariat of the authority, and any person appointed by formal decision of the authority) are competent to enter a private home without authorization of the inhabitant(s) upon explicit and specific authorization of the authority and notwithstanding the general conditions laid down in the Act on the Search of Private Homes (*Algemene Wet op het Binnentreden*) (Art 15 Dutch Act) (Art 58(6) GDPR).

## CLASS ACTIONS (ART 80 (2))



No Deviations

## ADMINISTRATIVE SANCTIONS (ART 83)



**SPECIFYING REQUIREMENT:** Administrative fines in Art 83(4)–(6) GDPR may also be imposed upon public authorities and bodies (Art 18(1) Dutch Act) (Art 83(7) GDPR).

## PENALTIES (ART 84)



**ADDITIONAL REQUIREMENT:** The supervisory authority is competent to impose the administrative fines of the GDPR (4% of worldwide turnover or €20 million) for violations of Art 10 GDPR (Art 18 Dutch Act) (Art 84 GDPR).

## HR PROCESSING (ART 88)



No Deviations

PROCESSING FOR ARCHIVING, SCIENTIFIC,  
HISTORICAL RESEARCH OR STATISTICAL  
PURPOSES (ART 89)

**ADDITIONAL REQUIREMENT:** When processing is carried out for archiving, scientific, historical, or research purposes, and the necessary safeguards are set in place, the controller can set aside the individual's rights to access, correction, and restriction of processing (Art 44 Dutch Act) (Art 89 GDPR). The prohibition to process sensitive data shall not apply when (1) this processing is necessary in light of scientific or historical research or statistical purposes; (2) this research serves a public purpose; (3) requesting consent is impossible or requires unreasonable effort; and (4) sufficient safeguards are provided to avoid harm to the individual's privacy rights (Art 24 Dutch Act) (Art 89 GDPR).

## OBLIGATIONS OF SECRECY (ART 90)



**VARYING REQUIREMENT:** Persons subject to an investigation by the authority cannot invoke an obligation of secrecy when cooperation is requested in light of that person's involvement in the investigation (Art 15(4) Dutch Act) (Art 90 GDPR).

## LOCAL DPA GUIDANCE &amp; LEGAL SOURCES



[Uitvoeringswet Algemene Verordening Gegevensbescherming](#)

[Local DPA Guidance on the Dutch Act](#)

## REMARKS

The Dutch Act contains procedural provisions governing the supervisory authority as well as substantive provisions.



## SPAIN

### NAME

# Proyecto de Ley Orgánica de Protec- ción de Datos de Carácter Personal

STATUS: DRAFT

### LAWFULNESS OF PROCESSING (ART 6)



**VARYING/ADDITIONAL REQUIREMENT:** The Spanish Act adopts specific requirements for data processing in specific sectors: (1) processing of data of an individual in a professional/business capacity is considered lawful under legitimate interests, provided the processor does not attempt to engage with the individual or process the data in other than a professional capacity (Art 19 Spanish Act); (2) the processing of personal data in the form of common credit system information is presumed lawful when this is carried out for purposes of monetary, financial, or credit obligations, upon certain conditions (Art 20 Spanish Act); (3) data processing for legitimate business purposes are presumed lawful when these are necessary for the continuation of the service (Art 21 Spanish Act); (4) CCTV is considered lawful when necessary for security purposes and upon strict conditions (Art 22 Spanish Act); (5) the creation of databases containing individuals who have expressed their right to opt out of receiving direct marketing is legitimate (Art 23 Spanish Act); and (6) whistleblowing hotlines are considered legitimate upon strict conditions (Art 24 Spanish Act) (Art 6 GDPR).

### CHILD'S CONSENT (ART 8)



**VARYING REQUIREMENT:** Minimum age to provide consent is lowered to 13 years old. Consent below that age shall only be valid when provided or authorized by the holder of parental responsibility or guardianship (Art 7 Spanish Act) (Art 8(1) GDPR).

### SENSITIVE DATA (GENETIC, BIOMETRIC AND HEALTH DATA) (ART 9(4))



**VARYING REQUIREMENT:** The prohibition on the processing of sensitive data cannot be lifted by the individual's consent when the main purpose remains the identification of the individual's ideology, union membership, religion, sexual orientation, beliefs, or racial or ethnic origin (Art 9(1) Spanish Act).

### CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)



No Deviations

### AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)



No Deviations

### RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)



**SPECIFYING REQUIREMENT:** When rightfully exercising a right to deletion, a data controller is required to block the individual's data. The blocked data will remain available to judges and courts, the public prosecutor, or competent public authorities, in particular competent supervisory authorities, for the determination of liability of the individual arising from the processing operation. The Spanish DPA and regional authorities may decide that such obligation to block the data does not apply when,

due to the high number of individuals affected and the nature of the data, this would pose a high risk to the rights of individuals concerned or would require a disproportionate effort from the data controller (Art 32 Spanish Act) (Art 23 GDPR).

### JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))



No Deviations

### AD HOC NOTIFICATIONS - RECORDS OF PROCESSING ACTIVITIES (ART 30)



**SPECIFYING REQUIREMENT:** Judicial authorities and public bodies are obligated to make public their record of processing (Art 31 Spanish Act) (Art 30 GDPR).

### SECURITY OF PROCESSING (ART 32)



No Deviations

### DATA BREACH (ART 33 & 34)



No Deviations

### DATA PROTECTION OFFICER (ART 37(4))



**ADDITIONAL REQUIREMENT:** The Spanish Act has provided for specific categories of companies that must appoint a DPO: (1) professional associations and general councils; (2) schools and public and private universities; (3) telecom providers and network operators; (4) information society service providers; (5) entities supervising credit institutions; (6) credit institutions; (7) insurance companies; (8) investment service companies; (9) gas and electricity providers; (10) credit rating and fraud prevention entities; (11) entities carrying out advertising and commercial prospecting (market research); (12) health institutions required to maintain patient





## SPAIN

records; (13) the gambling and gaming sector; and (14) the private security sector (Art 34 Spanish Act) (Art 37(4) GDPR).

## DATA TRANSFER DEROGATIONS (ART 49(5))



No Deviations

## POWERS SUPERVISORY AUTHORITIES (ART 58)



**SPECIFYING/ADDITIONAL REQUIREMENT:** The Spanish Act foresees that investigatory competencies include contacting the relevant public authority in Spain to obtain evidence of the data protection violation and identification by telecom and information society services providers. In addition, they may obtain all information for the fulfillment of their duties, conduct inspections, require the delivery of evidence or other documents, obtain copies thereof, and inspect hardware and IT systems (Art 52 Spanish Act). They may also carry out searches on (private) homes in accordance with procedural rules governing these searches (e.g., upon prior judicial authorization) (Art 53 Spanish Act). The DPA may also carry out preventive audits (Art 54 Spanish Act). During an investigation, the individual or entity under investigation has a duty to cooperate (Art 52 Spanish Act).

Furthermore, the president of the DPA shall have the power to issue implementing legislation called "circulars" that will become binding after publication in the *Official Gazette* (Art 55 Spanish Act). There may also be regional DPAs, supervised by the Spanish DPA, appointed to exercise the powers of a supervisory authority granted by the GDPR (Art 57–58 Spanish Act) (Art 58 GDPR).

## CLASS ACTIONS (ART 80 (2))



No Deviations

## ADMINISTRATIVE SANCTIONS (ART 83)



**SPECIFYING/ADDITIONAL REQUIREMENT:** The Spanish Act categorizes infringements as "very serious," "serious," and "mild." Very serious infringements are, in addition to the GDPR: (1) processing of personal data related to criminal offenses

outside GDPR limits; (2) processing of administrative personal data outside the limits of the Spanish Act; (3) breach of the secrecy obligation imposed on controllers and processors by the Spanish Act; (4) failure to lock the data pursuant to the Spanish Act; and (5) inhibiting the data protection investigation by the Spanish DPA or other competent authority. In these cases, the statute of limitations is three years (Art 72 Spanish Act).

Serious infringements include lack of cooperation in procedures of the supervisory authorities (not under Art 72) (Art 73 Spanish Act). In these cases, the statute of limitations is two years.

The most important mild infringements include: (1) infringements against the information obligation; (2) failure to respond to individual rights requests without justification; (3) failure to comply with the notification requirement of access or correction request; (4) failure to delete the data pursuant to the Spanish Act; (5) violations of controller/processor responsibilities pursuant to controller/processor agreements; and (6) failure to comply with all requirements of recordkeeping (ad hoc notifications). In these cases, the statute of limitations is one year (Art 74 Spanish Act).

The Spanish Act also allows for a suspension and interruption of the statute of limitations (causing a potential restart of the limitation period) (Art 75 Spanish Act). A potential aggravating factor, in addition to those mentioned in the GDPR, may exist in the continuous nature of the infringement (Art 76 Spanish Act). In case the entity sentenced is a legal person, an additional sanction may exist in the publication of the judgment (including revealing the identity of the entity sentenced) in the *Official Gazette* (Art 76(4) Spanish Act). Additionally, statutes of limitations are set at one year for fines of less than €40,000, at two years for fines between €40,001 and €300,000, and at three years for fines exceeding €300,000.

## PENALTIES (ART 84)



No Deviations

## HR PROCESSING (ART 88)



No Deviations

## PROCESSING FOR ARCHIVING, SCIENTIFIC, HISTORICAL RESEARCH OR STATISTICAL PURPOSES (ART 89)



**SPECIFYING REQUIREMENT:** For data processing for statistical purposes, competent bodies may deny individuals their access, correction, deletion, objection, restriction, portability, and automated decision-making rights when the data are covered by the statistical confidentiality guarantees provided in state or regional legislation (Art 25 Spanish Act) (Art 89 GDPR). For data processing for archiving purposes, this shall only be lawful when carried out for purposes of the public interest described in specific Spanish legislation or the GDPR (Art 26 Spanish Act) (Art 89 GDPR).

## OBLIGATIONS OF SECRECY (ART 90)



**SPECIFYING REQUIREMENT:** The Spanish Act sets forth an obligation of secrecy for controllers and processors (as well as all other persons involved) for data processing activities. These are in addition to any obligations of professional secrecy that may apply. The obligation remains even when the contractual relationship of the controller-processor has ended (Art 5 Spanish Act) (Art 90 GDPR).

## LOCAL DPA GUIDANCE &amp; LEGAL SOURCES



[Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal](#)

## REMARKS

The Spanish Act foresees procedural rules governing proceedings before the Spanish DPA, as well as substantive provisions.



## UNITED KINGDOM

NAME

### Data Protection Bill

STATUS: ADOPTED

#### LAWFULNESS OF PROCESSING (ART 6)



No Deviations

#### CHILD'S CONSENT (ART 8)



**VARYING REQUIREMENT:** Minimum age to provide consent is lowered to 13 years old. Art 8 GDPR is not applicable to preventive and counseling services (Clause 8 UK Bill) (Art 8(1) GDPR).

#### SENSITIVE DATA (GENETIC, BIOMETRIC AND HEALTH DATA) (ART 9(4))



No Deviations

#### CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)



**SPECIFYING REQUIREMENT:** Processing of this type of data is allowed other than under control of an official authority and only if one of the following conditions are met: (1) consent; (2) protecting the individual's vital interests; (3) processing by not-for-profit bodies; (4) personal data is in the public domain; (5) legal claims or when a court is acting in its judicial capacity; (6) indecency offenses involving children; or (7) substantial public interest condition (Clauses 9(4), (5) and Schedule 1, Part 3 UK Bill).

#### AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)



No Deviations

#### RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)



**SPECIFYING REQUIREMENT:** Most data subjects' rights can be restricted when processing occurs for the following purposes: (1) crime and taxation (including risk assessment systems); (2) maintenance of effective immigration control; (3) the legal requirement to disclose information or in the context of legal proceedings; (4) discharging a function to protect the public; (5) discharging regulatory functions relating to legal, health, and children's services; (6) functions of certain other regulatory bodies; (7) avoiding infringement of parliamentary privilege; (8) assessing a person's suitability for judicial appointment or in the context of judicial independence and judicial proceedings; (9) in the context of Crown honors, dignities, and appointments; (10) protection of the rights of others; (11) legal professional privilege; (12) avoiding self-incrimination; (13) corporate finance service; (14) prejudiced business activity; (15) negotiations between the data subject and controller; (16) confidential references given to the controller; (17) information recorded in the context of exams; (18) incompatibility with the publication of journalistic, academic, literary, or artistic material in the public interest; (19) statistical or scientific and historical, or archiving in the public interest, in the case of health, social work, and education data; (20) when the data are processed by a court; (21) as a result of the data subject's expectations or wishes; (22) when disclosure would lead to serious harm (for health data); (23) when an appropriate professional must give prior opinion, in the case of child abuse data; (24) when it would not be in the best interests of the data subject to disclose; (25) human fertilization and embryology information; (26) adoption records and reports;

(27) statements of special educational needs; (28) parental order records and reports; and (29) information provided in the context of the Children's Hearings Act (Clause 14 and Schedules 2-4 UK Bill).

#### JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))



No Deviations

#### AD HOC NOTIFICATIONS - RECORDS OF PROCESSING ACTIVITIES (ART 30)



**ADDITIONAL REQUIREMENT:** A record maintained by a controller or processor under Article 30 for the processing of data that requires an appropriate policy document must include the following information: (1) which condition is relied on; (2) to what extent processing is lawful under Art 6 GDPR; and (3) the erasure/retention policy and, where applicable, reasons for not complying with this policy.

#### SECURITY OF PROCESSING (ART 32)



**VARYING REQUIREMENT:** Article 32 GDPR does not apply when processing for national security or defense purposes (Clause 26 UK Bill).

#### DATA BREACH (ART 33 & 34)



**VARYING REQUIREMENT:** There is no notification obligation to the data protection commissioner when: (1) the data breach also constitutes a relevant error within the meaning of Section 231(9) of the Investigatory Powers Act 2016 (Clause 106(6) UK Bill); (2) a crime can be prevented or detected; (3) information is required to be disclosed to the public by law; (4) there is infringement of parliamentary privilege; (5) the breach is likely to prejudice judicial proceedings; and (6) Crown honors and dignities are



## UNITED KINGDOM

at risk. There is also no notification obligation when the following is at risk or prejudiced: (7) the armed forces; (8) the economic well-being of the UK; (9) legal professional privilege; and (10) negotiations with the data subject. There is also no notification obligation when the personal data concerned relates to: (11) confidential references by the controller; (12) exams and marks; (13) research and statistics; and (14) archiving in the public interest (Schedule 11 UK Bill).

It is required to communicate the nature of a data breach to the data subject (Clause 66(2) (a) UK Bill). The controller may restrict communication of this information to the data subject when it is necessary and proportionate to avoid obstruction of an official or legal inquiry, investigation, or procedure; to avoid prejudice of prevention and detection of criminal offenses or execution of criminal penalties; or to protect public or national security or the rights and freedoms of others (Clause 66(7) UK Bill).

## DATA PROTECTION OFFICER (ART 37(4))



**VARYING REQUIREMENT:** An exception for designation of a DPO is also made for “other judicial authorities” (i.e., other than courts) acting in their judicial capacity (Clause 67(1) UK Bill). Clause 69(2) UK Bill lays down a nonexhaustive list of specific tasks to be performed by the DPO when monitoring compliance with controller policies.

## DATA TRANSFER DEROGATIONS (ART 49(5))



No Deviations

POWERS SUPERVISORY AUTHORITIES  
(ART 58)

**VARYING REQUIREMENT:** The commissioner’s powers under the GDPR are subject to safeguards provided for in the UK Bill: (1) powers over information requests are exercisable only upon written information notice by the commissioner to the controller/processor; (2) investigatory powers and powers allowing access to premises and personal data are exercisable only upon a written assessment notice (and the results of the assessment must be communicated, see Clause 125(2) UK Bill); (3) powers to order compliance with the data subject’s requests, to render processing compliant, to communicate a breach to the data subject, to impose a limitation or ban on processing activities, to order the rectification or erasure of personal data, and to withdraw a certification are exercisable only upon enforcement notice; (4) the power to impose an administrative fine is exercisable only upon penalty notice (Clause 113 UK Bill). The commissioner has the power to inspect personal data in accordance with international obligations (Clause 117 UK Bill). The commissioner has the power to issue information, assessment, enforcement, and penalty notices (Clauses 137–146 and 148–152 UK Bill). The commissioner’s powers of entry and inspection may only be exercised upon court approval or warrant (Schedule 15 UK Bill).

## CLASS ACTIONS (ART 80(2))



**VARYING REQUIREMENT:** The UK Bill omits Art 80(2) GDPR (see Schedule 6, Part 1, Clause 53(b) UK Bill).

## ADMINISTRATIVE SANCTIONS (ART 83)



No Deviations

## PENALTIES (ART 84)



No Deviations

## HR PROCESSING (ART 88)



**VARYING REQUIREMENT:** The UK Bill omits Art 88 GDPR (see Schedule 6, Clause 61 UK Bill).

PROCESSING FOR ARCHIVING, SCIENTIFIC,  
HISTORICAL RESEARCH OR STATISTICAL  
PURPOSES (ART 89)

**VARYING REQUIREMENT:** The UK Bill restricts the derogations made according to Art 89(2) GDPR for processing for research and statistics purposes to Art 15(1)–(3), Art 16, Art 18(1), and Art 21(1) GDPR. The UK Bill restricts the derogations made according to Art 89(3) GDPR for processing for archiving purposes to Art 15(1)–(3), Art 16, Art 18(1), Art 19, Art 20(1), and Art 21(1) GDPR.

## OBLIGATIONS OF SECRECY (ART 90)



No Deviations

## LOCAL DPA GUIDANCE AND LEGAL SOURCES



[Data Protection Bill](#)

[Factsheet Data Protection Bill](#)

## REMARKS

The UK Data Protection Bill also contains processing activities that do not fall within EU law or the GDPR, such as processing related to immigration and national security and parts implementing the EU Law Enforcement Directive.