AUSTRIA

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

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

STATUS: ADOPTED

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

CHILD'S CONSENT (ART 8)

✓

SPECIFYING PROVISION:

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 Deviation

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 Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

RESTRICTING PROVISIONS:

1. **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 Deviation

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 REQUIREMENT:

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).

DATA BREACH (ART 33 & 34)

No Deviation

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 Deviation

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))

SPECIFYING PROVISIONS:

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 Deviation

HR PROCESSING (ART 88)

SPECIFYING PROVISION:

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).

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

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 & LEGAL SOURCES

DATA PROTECTION AMENDMENT ACT 2018

BELGIUM

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Wet tot Oprichting van de Gegevensbeschermingsautoriteit

STATUS: ADOPTED

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

CHILD'S CONSENT (ART 8)

✗

No Deviation

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

✗

No Deviation

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

✗

No Deviation

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

✗

No Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

✗

No Deviation

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

✗

No Deviation

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

✗

No Deviation

SECURITY OF PROCESSING (ART 32)

✗

No Deviation

DATA BREACH (ART 33 & 34)

✗

No Deviation

DATA PROTECTION OFFICER (ART 37(4))

✗

No Deviation

DATA TRANSFER DEROGATIONS (ART 49(5))

✗

No Deviation

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 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 Deviation

HR PROCESSING (ART 88)

No Deviation

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

No Deviation

OBLIGATIONS OF SECRECY (ART 90)

No Deviation

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.

CROATIA

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Zakon O Provedbi Opce Uredbe O Zastiti Podataka

STATUS: ADOPTED

SME EXCEPTION

✗

No Deviation

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

CHILD'S CONSENT (ART 8)

✓

SPECIFYING REQUIREMENT:

1. **Age:** A user must be at least 16 years old to consent to information society services directed at children (Art 19(1) Croatian Act).
2. **Territorial Scope of Application:** It is explicitly set forth that the consent rule shall apply to a child resident in Croatia (Art 19(2) Croatian Act).

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

✓

DEVIATING REQUIREMENT:

1. **Genetic Data Processing:** The processing of genetic data to assess health conditions for the purpose of life insurance contracts is prohibited. The prohibition cannot be lifted with the consent of the data subject (Art 20(1) Croatian Act). This applies to data subjects concluding life insurance agreements in Croatia with a data controller that is established in Croatia or provides services there (Art 20(4) Croatian Act).
2. **Biometric Data Processing:** Public authorities and private companies may process biometric data if (1) there is a legal basis for it; (2) it is necessary to protect natural persons, confidential information, or trade secrets; and (3) the interests of the data subject involved have been taken into account (Art 21(1) Croatian Act). Public authorities may also process biometric data when it is necessary for border control (Art 21(2) Croatian Act).
3. **Employee Biometric Data Processing:** The processing of biometric data of employees is allowed for the purpose of monitoring employment performance (working hours) and access control (company premises) if there is a legal basis for it or the employee gives explicit consent and the biometric data processing serves as an alternative to other means of performing these types of monitoring (Art 23 Croatian Act).

4. **Territorial Application of Biometric Data Processing:** The provisions on biometric data processing in the Croatian Act apply to data subjects if processing is carried out by a data controller that is established or providing services in Croatia or by a public authority (Art 24(1) Croatian Act). They do not apply to public defense, national security, and national intelligence services (Art 24(3) Croatian Act).

CCTV (ART 6)

ADDITIONAL REQUIREMENT:

1. **General Scope and Purposes:** The processing of personal data through video surveillance can only be carried out for security reasons and to the extent overriding interests of the data subject do not prevail (Art 26(1) Croatian Act). Video surveillance may cover the inside and external façade of a building, parts of a building, and inside public transportation (Art 26(2) Croatian Act).
2. **Notice:** The controller or processor is responsible for signage indicating which parts of the premises are under video surveillance. This signage should be put up and made clear to the data subject at the latest when entering the area under video surveillance (Art 27(1) Croatian Act). This signage should contain all information required in light of transparency under the GDPR, but in particular an easily understandable pictogram with the following: (1) the fact that the space is under surveillance; (2) information about the controller; and (3) contact information through which the data subject can exercise his rights (Art 27(2) Croatian Act).
3. **Security and Data Subject Rights:** The CCTV images must be subject to access control to restrict access to authorized persons (the controller and processor are responsible for setting up a system that logs date and time stamps of each access to the CCTV images and who has obtained access). Competent authorities will be granted access to CCTV images in the context of the exercise of their duties (Art 28 Croatian Act).
4. **Retention Period:** Records obtained through CCTV can be stored for a maximum of six months unless an applicable law prescribes a longer retention term or if the records are evidence in judicial, administrative, or arbitration proceedings (Art 29 Croatian Act).
5. **CCTV in the Workplace:** This is permitted provided applicable health and safety regulations are taken into account and the employees were adequately informed of the use of CCTV. CCTV cannot cover changing rooms, relaxation and resting areas, or bathrooms (Art 30 Croatian Act).
6. **CCTV in Residential Buildings:** To the extent a residential or commercial property is subject to co-ownership, two-thirds of co-owners must agree to the installation of a CCTV system in order for it to be placed. Only entrances, exits, and common areas can be covered by the CCTV (Art 31 Croatian Act).
7. **CCTV in Public Areas:** This is only permitted when carried out by public authorities, when it is prescribed by law and necessary for the performance of tasks of the public authority, or for public interests (Art 32 Croatian Act).

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

No Deviation

INFORMATION OBLIGATION (ART 13 & 14)

No Deviation

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

No Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

DEVIATING REQUIREMENT:

Processing for Statistical Purposes: When personal data is processed by public bodies for the purpose of producing statistics, such bodies are not obliged to grant rights of access, correction, processing restrictions, or objection when this is strictly necessary in light of statistics. In addition, data controllers are not required to inform data subjects about data transfers when necessary for statistical purposes (Art 33 Croatian Act).

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

No Deviation

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

No Deviation

SECURITY OF PROCESSING (ART 32)

No Deviation

DATA BREACH (ART 33 & 34)

No Deviation

DATA PROTECTION IMPACT ASSESSMENT (ART 35)

No Deviation

DATA PROTECTION OFFICER (ART 37(4))

No Deviation

CERTIFICATION (ART 42)

SPECIFYING REQUIREMENT:

Accreditation: The national accreditation body designated on the basis of Regulation (EC) No. 765/2008 for accreditation and marketing surveillance relating to the marketing of products shall be responsible for accreditation of certification bodies (Art 5 Croatian Act).

DATA TRANSFER DEROGATIONS (ART 49(5))

No Deviation

POWERS SUPERVISORY AUTHORITIES (ART 58)

SPECIFYING REQUIREMENT:

1. **Initiation:** A procedure before the Croatian supervisory authority may be initiated upon individual request. The authority shall make a decision on this request (against which no appeal can be filed) (Art 34 Croatian Act).
2. **Removal of Data:** To the extent the deletion/removal of data is ordered, disproportionate deletion/removal can be contested (Art 35 Croatian Act).
3. **Investigation:** On-site investigations may be carried out by the authority; its members will present proof of identification when they perform the investigation. The authority may request assistance from the Ministry of Internal Affairs to the extent there is resistance to the investigation (Art 36 Croatian Act). The authority may make all copies and duplications and collect all other information it deems necessary. It can also seize storage systems or equipment for a maximum period of 15 days or seal those systems when strictly necessary. In those instances, it will draw up an official report detailing the need for these measures (Art 37 Croatian Act). The authority will also draw up minutes of the entire investigation detailing the course of action of the investigation (Art 40 Croatian Act).
4. **Confidential Data:** Data covered by confidentiality (such as legal privilege) pursuant to a specific legislative regime will only be copied or accessed by the authority in line with that regime and will be accessed in the presence of public officials who are certified to access that data (Art 38 Croatian Act).

CLASS ACTIONS (ART 80 (2))

No Deviation

ADMINISTRATIVE SANCTIONS (ART 83)

ADDITIONAL REQUIREMENT:

1. **No Appeal:** The Croatian supervisory authority determines the amount and payment modalities of the administrative fine in a decision, which is not open to appeal with the authority. The defendant may, however, commence proceedings before the competent administrative court (Art 45 Croatian Act).
2. **Seizure:** To the extent the defendant refrains from payment of the administrative fine imposed on it in due course, the authority may inform the competent Regional Office of Tax Administration, which is authorized to obtain payment through seizure (Art 46 Croatian Act).
3. **Exception for Public Authorities:** No administrative fines may be imposed on public authorities (Art 47 Croatian Act).
4. **CCTV Fines:** Controller and/or processors can be fined 50,000.00 HRK if (1) they do not indicate which parts of the premises are covered by CCTV; (2) no automatic recording/logging system is installed that logs access to CCTV recordings; and (3) CCTV recordings are used for purposes other than those mentioned in the Croatian Act (Art 51 Croatian Act).

PENALTIES (ART 84)

No Deviation

FREEDOM OF EXPRESSION & INFORMATION (ART 85)

No Deviation

HR PROCESSING (ART 88)

No Deviation

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

DEVIATING REQUIREMENT:

Statistical Data Processing: Data must be de-identified when included in statistical reports (Art 33 Croatian Act).

OBLIGATIONS OF SECRECY (ART 90)

ADDITIONAL REQUIREMENT:

SA Members: Officials and directors of the Croatian supervisory authority itself will be subject to fines if they do not respect the obligation to keep secret any confidential information they learn in the performance of their function at the authority.

LOCAL DPA GUIDANCE & LEGAL SOURCES

Croatian Data Protection Act

CYPRUS

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Ο περί της Προστασίας των Φυσικών Προσώπων Έναντι της Επεξεργασίας των Δεδομένων Προσωπικού Χαρακτήρα και της Ελεύθερης Κυκλοφορίας των Δεδομένων αυτών Νόμος του 2018 (N. 125(I)/2018)

STATUS: ADOPTED

SME EXCEPTION

✗

No Deviation

LAWFULNESS OF PROCESSING (ART 6)

✓

VARYING:

Exception added for courts of Cyprus during their operations; and the Cypriot parliament during its operations.

CHILD'S CONSENT (ART 8)

✓

SPECIFYING:

14 years old

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

✓

VARYING:

Prohibition of processing genetic or biometric data for life insurance or medical insurance purposes.

CCTV (ART 6)

✗

No Deviation

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

VARYING:

When public bodies combine two or more databases that contain a large number of personal data relating to criminal convictions, they need to first conduct a DPIA and consult with the Cypriot data protection commissioner.

INFORMATION OBLIGATION (ART 13 & 14)

Information obligations are applicable to the extent they do not violate the freedom of expression or the freedom of journalism.

AUTOMATED INDIVIDUAL DECISION MAKING (ART 22)

No Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

ADDITIONAL:

In order for a data controller or processor to invoke an Article 23 exception, they need to first conduct a DPIA and consult with the Cypriot data protection commissioner. The data protection commissioner can impose conditions on any such restriction.

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

No Deviation

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

ADDITIONAL:

The following aspects of records of processing activities are a criminal offense:

- Not having a record of processing activities.
- Having but not updating a record of processing activities.
- Having but not providing a record of processing activities to the authorities upon request.
- Providing an outdated, inaccurate, or incomplete record of processing activities to the authorities.

SECURITY OF PROCESSING (ART 32)

No Deviation

DATA BREACH (ART 33 & 34)

VARYING:

It is a criminal offense not to notify the Supervisory Authority about a data breach. It is a criminal offense not to notify the data subject about a data breach.

DATA PROTECTION IMPACT ASSESSMENT (ART 35)

VARYING:

It is a criminal offense not to conduct a data protection impact assessment.

DATA PROTECTION OFFICER (ART 37(4))

No Deviation

CERTIFICATION (ART 42)

VARYING:

It is a criminal offense for a certification body to provide a certificate that does not fulfill all the GDPR Article 42 requirements.

DATA TRANSFER DEROGATIONS (ART 49(5))

ADDITIONAL:

A DPIA and previous consultation with the SA is required for every data transfer derogation.

POWERS OF SUPERVISORY AUTHORITIES (ART 58)

✓

ADDITIONAL:

The SA has the following additional authorities:

- Access to any personal data requested for any reason without any confidentiality claim (excluding the client-lawyer legal privilege).
- Dawn raid in any establishment (excluding houses).
- Engage forensic experts and/or the police forces for any of its functions.
- Confiscate any relevant documents and equipment.
- Require the Cypriot Organization for the Promotion of Quality to revoke any certification.
- To report the Cypriot Organization for the Promotion of Quality to the European Commission for noncompliance.
- Impose conditions on a number of GDPR functions.
- Report to the police and the criminal prosecutor any noncompliance that may amount to a criminal offense.
- Be in charge of staff member transfers.

CLASS ACTIONS (ART 80(2))

✗

No Deviation

ADMINISTRATIVE SANCTIONS (ART 83)

✓

SPECIFYING:

Administrative sanction to a public body regarding not-for-profit processing activities cannot be higher than €200,000.

PENALTIES (ART 84)

✓

SPECIFYING:

Depending on the GDPR violation, criminal penalties range from 1–5 years of imprisonment and €10,000–50,000.

FREEDOM OF EXPRESSION AND INFORMATION (ART 85)

✗

No Deviation

HR PROCESSING (ART 88)

✗

No Deviation

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

✗

No Deviation

OBLIGATIONS OF SECRECY (ART 90)

✗

No Deviation

LOCAL DPA GUIDANCE AND LEGAL SOURCES

✓

The Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of such Data Act of 2018 (Law 125 (I) / 2018)

CZECH REPUBLIC

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Návrh zákon o zpracování osobních údajů

STATUS: DRAFT

SME EXCEPTION

✗

No Deviation

LAWFULNESS OF PROCESSING (ART 6)

✓

SPECIFYING PROVISION:

Processing for New Purposes: Controllers can process personal data for purposes other than collection if necessary to meet a legal obligation or when this is in the public interest, or in the exercise of public powers, such as: (1) public policy and internal security; (2) defense or security of the Czech Republic; (3) prevention, detection, and prosecution of criminal offenses or for the execution of judgments; (4) public policy objectives of the EU; (5) protection of judiciary independence; (6) prevention, detection, and prosecution of ethical rules of regulated professions; (7) exercise of official authority; (8) protection of individuals' rights and freedoms; and (9) the enforcement of civil claims (Art 5 Czech Act).

CHILD'S CONSENT (ART 8)

✓

SPECIFYING PROVISION:

For information society services offered directly to children, consent within the meaning of Art 6(1)(a) GDPR is valid if the child is 13 years of age or if this is expressed or approved by the child's legal representative (Art 6 Czech Act).

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

✗

No Deviation

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

✗

No Deviation

INFORMATION OBLIGATION (ART 13 & 14)

SPECIFYING PROVISION:

Information may be made available to the data subject via publication by remote access if the controller performs processing on the basis of a legal obligation or in the public interest or if the controller conducts processing in the exercise of public authority (Art 7 Czech Act).

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

No Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

ADDITIONAL REQUIREMENT:

1. **Right of Access:** The right of access may be limited or excluded if it is necessary and proportionate in light of the protection of another individual's rights (Art 10 Czech Act).
2. **Right to restriction of processing:** The right to restriction of processing may be limited or excluded when the controller or processor is under a legal obligation to transfer the data or make it available (Art 12 Czech Act).

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

No Deviation

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

No Deviation

SECURITY OF PROCESSING (ART 32)

No Deviation

DATA BREACH (ART 33 & 34)

No Deviation

DATA PROTECTION IMPACT ASSESSMENT (ART 35)

SPECIFYING PROVISION:

The controller does not need to perform DPIAs before beginning processing activities unless this is explicitly provided for by law (Art 9 Czech Act).

DATA PROTECTION OFFICER (ART 37(4))

SPECIFYING PROVISION:

DPO appointment requirement: The requirement to appoint a DPO when processing is carried out by a public body is specified by the interpretation of "public body," which shall be considered a statutory body carrying out statutory tasks in the public interest (Art 13 Czech Act).

CERTIFICATION (ART 42)

No Deviation

DATA TRANSFER DEROGATIONS (ART 49(5))

No Deviation

POWERS SUPERVISORY AUTHORITIES (ART 58)

SPECIFYING PROVISION:

1. **Powers:** The supervisory authority's powers shall include: performing investigations and audits, notifying controller/processor of infringements (which in turn may request clarification), establishing criteria for data protection certificates, approving codes of conduct, adopting standard contractual clauses, and imposing corrective measures to remedy data protection law infringements. If, however, an infringement is remedied immediately after discovery of the infringement, the supervisory authority can waive the imposition of a fine (Art 50 and 57–58 Czech Act).
2. **Cooperation:** The supervisory authority shall cooperate with the EDPS, EU institutions, and other Member States' supervisory authorities. It shall comply with requests for information, investigations, or audits from other supervisory authorities (Art 50 Czech Act).
3. **Confidentiality:** Members of the supervisory authority are bound to confidentiality of data the disclosure of

which would jeopardize the personal data concerned. This duty of confidentiality persists after termination of the employment relationship and can only be lifted in legal proceedings, with the consent of the individual whose personal data is concerned and protected by the duty of confidentiality (Art 56 Czech Act).

CLASS ACTIONS (ART 80 (2))

No Deviation

ADMINISTRATIVE SANCTIONS (ART 83)

ADDITIONAL REQUIREMENT:
Fines imposed on public authorities: Public authorities acting as controller or processor that are in violation of the Czech Act can be fined up to 10 million CZK (€39,310) (Art 61 Czech Act).

PENALTIES (ART 84)

No Deviation

FREEDOM OF EXPRESSION AND INFORMATION (ART 85)

ADDITIONAL REQUIREMENT: For processing carried out for journalistic or academic purposes, the Czech Act foresees the following specifications and exemptions:

1. **Sensitive data processing:** Only allowed for journalistic or academic purposes if necessary to achieve the legitimate objective pursued and where the individual's rights do not prevail.
2. **Criminal data processing:** Identical to sensitive data processing.
3. Information obligation and other individual rights: The controller may postpone making available the identity of the source and content of the personal information and may limit or exclude the individual's rights for as long as necessary to achieve the journalistic or academic processing purpose. The individual may only exercise his right to restriction of processing when this is necessary for the exercise and defense of legal claims and must be balanced with the right to information and freedom of expression. The individual may object to processing if he demonstrates his interests prevail (Art 15 Czech Act).

HR PROCESSING (ART 88)

No Deviation

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

No Deviation

OBLIGATIONS OF SECRECY (ART 90)

SPECIFYING PROVISION: Information protected by legal privilege can only be accessed and consulted by the supervisory authority in the presence and with the consent of a representative of the Czech Bar (Art 54 Czech Act).

LOCAL DPA GUIDANCE & LEGAL SOURCES

CZECH DATA PROTECTION ACT

REMARKS

The Czech Act also contains data processing by competent authorities for purposes of law enforcement and public security, which is out of scope of the GDPR.

DENMARK

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Forslag til Lov om Supplerende Bestemmelser til Forordning om Beskyttelse af Fysiske Personer i Forbindelse med Behandling af Personoplysninger og om fri Udveksling af Sådanne Oplysninger (databeskyttelsesloven)

STATUS: ADOPTED

SME EXCEPTION

✗

No Deviation

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

CHILD'S CONSENT (ART 8)

✓

VARYING REQUIREMENT:

Minimum age lowered: Minimum age to provide consent is lowered to 13 years (Ch 3, § 6 Danish Act).

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

✗

No Deviation

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

✓

VARYING REQUIREMENT:

Information Systems in the Public Interest: Processing personal data relating to criminal convictions and offenses is permitted if done solely for providing information systems with significant public benefit and when the processing is necessary for implementation of the systems. This information may not be disclosed to or processed by credit information agencies (Ch 3, § 9; Ch 4, § 15; Ch 5, § 20 Danish Act).

INFORMATION OBLIGATION (ART 13 & 14)

✓

VARYING REQUIREMENT:

Exception to Transparency Requirement: A data controller does not need to provide notice to data subjects if this is in the interest of the data subject or another natural person (Ch 6, § 22 Danish Act).

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

✗

No Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

✓

SPECIFYING REQUIREMENT:

1. Exception for Public Administration: Information processed for public administration as part of administrative cases may be exempted from the right of access in accordance with the Danish Public Administration Act.

2. Exception for Courts: The right of information and access shall not apply to the processing of personal data made to the courts when they act in their capacity as courts.

3. Exception for Scientific and Statistical Processing: Rights of access, correction, restriction, and objection shall not apply if the information is exclusively processed for scientific or statistical purposes.

4. Exception for Criminal Investigation: There is no obligation for the controller to notify the data subject of a data breach if the notification of data subjects interferes with a criminal investigation as determined by the police.

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

✗

No Deviation

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

✗

No Deviation

SECURITY OF PROCESSING (ART 32)

✗

No Deviation

DATA BREACH (ART 33 & 34)

✗

No Deviation

DATA PROTECTION IMPACT ASSESSMENT (ART 35)

✗

No Deviation

DATA PROTECTION OFFICER (ART 37(4))

✓

VARYING REQUIREMENT:

Confidentiality: Data protection officers shall not unlawfully disclose or exploit information that they have become aware of in the performance of their duties (Ch 7, § 24 Danish Act).

CERTIFICATION (ART 42)

✗

No Deviation

DATA TRANSFER DEROGATIONS (ART 49(5))

✗

No Deviation

POWERS SUPERVISORY AUTHORITIES (ART 58)

✓

VARYING REQUIREMENT:

No Appeal Before Administrative Authority: The Data Inspectorate's decisions cannot be appealed before another administrative authority (Ch 10, § 30 Danish Act).

CLASS ACTIONS (ART 80 (2))

✗

No Deviation

ADMINISTRATIVE SANCTIONS (ART 83)

✗

No Deviation

PENALTIES (ART 84)

VARYING REQUIREMENT:
Criminal Penalties: Because the legal system of Denmark does not allow for administrative fines, the Danish Act provides for criminal penalties for violations of the GDPR, including fines or imprisonment for up to six months (Ch 12, § 41 Danish Act).

FREEDOM OF EXPRESSION & INFORMATION (ART 85)

No Deviation

HR PROCESSING (ART 88)

No Deviation

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

VARYING REQUIREMENT:

Archiving: Information covered by the Danish Act may be transferred to archive storage in accordance with the rules of the Archive Act (Ch 3, § 14 Danish Act).

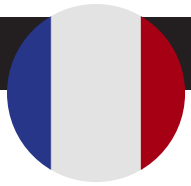
OBLIGATIONS OF SECRECY (ART 90)

VARYING REQUIREMENT:

DPO Obligation of Secrecy: Data protection officers that unlawfully disclose or exploit information obtained in the performance of their duties shall be fined, unless higher punishment is allowed by other legislation (Ch 12, § 41(4) Danish Act).

LOCAL DPA GUIDANCE & LEGAL SOURCES

Danish Data Protection Act



FRANCE

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Project de loi relatif à la protection des données personnelles

STATUS: DRAFT

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

CHILD'S CONSENT (ART 8)

✗

No Deviation

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 Deviation

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 Deviation

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 Deviation

DATA BREACH (ART 33 & 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 Deviation

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 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 Deviation

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 Deviation

PENALTIES (ART 84)

✘

No Deviation

HR PROCESSING (ART 88)

✘

No Deviation

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 Deviation

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

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

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 Deviation

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 Deviation

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).
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 Deviation

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

No Deviation

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))

SPECIFYING PROVISIONS:

1. Controllers & Processors: Both controllers and processors are subject to DPO obligations.

2. Duty to Appoint: Companies must appoint a DPO whenever:

a. They employ at least 10 people whose regular duties include processing personal data;

b. Their usual business includes processing data for purposes of transferring the data (e.g., data brokers), transferring the data anonymously, or market or opinion research; or

c. They conduct processing that requires a Data Protection Impact Assessment (DPIA) under Article 35 GDPR.

See § 38 BDSG-New.

3. Protected Employment:

a. DPOs cannot be fired unless employers can show facts that would permit the employee's immediate termination for cause.

b. Internal DPOs who leave the DPO position maintain protected employment status for one year.

See § 6 BDSG-New.

4. Protected DPO Status:

A DPO cannot be removed from their position of DPO (even if not fired from the organization) unless the employer can show facts analogous to what would permit immediate termination for cause.

See § 6 BDSG-New.

For more details, see: An English-Language Primer on Germany's GDPR Implementation Statute: Part 3 of 5

DATA TRANSFER DEROGATIONS (ART 49(5))

No Deviation

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 Deviation

ADMINISTRATIVE SANCTIONS (ART 83)

SPECIFYING PROVISIONS:

1. Fines: FFor 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.

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)

GREECE

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Νόμος για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα ("Law for the Protection of Personal Data")

STATUS: DRAFT

LAWFULNESS OF PROCESSING (ART 6)

✓

VARYING REQUIREMENT: Additional provisions regarding CCTV processing, namely scope of applicability of CCTV processing, requirements that render such processing lawful, exceptions, data retention requirements, data transfers, and DPO duties and notification requirements (Art 5 Greek Law).

CHILD'S CONSENT (ART 8)

✓

VARYING REQUIREMENT: Minimum age to provide consent is lowered to 15 years (Art 6 Greek Law).

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

✓

VARYING REQUIREMENT: Sensitive data cannot be processed for health or life insurance purposes. This prohibition also extends to broader family members (i.e., it is forbidden to process sensitive data of the parent to determine the health or life insurance particulars of the child) (Art 7 Greek Law).

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

✓

SPECIFYING REQUIREMENT: Data processing of criminal convictions is allowed when it is absolutely necessary for the following purposes: (1) determination of eligibility to run in elections, or for job employment purposes; (2) processing data in the employment context; (3) archiving or other public utility purposes; (4) freedom of expression; and (5) the establishment, exercise, or defense of legal claims (Art 8 Greek Law).

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

✗

No Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

ADDITIONAL REQUIREMENT:

Restrictions to the right of information and access: The data controller can refuse the right to access when the data relates to national security; public defense; crime prevention; important economic or financial interests; establishment, exercise, or defense of legal claims; and the protection of the data subject or the rights and freedoms of others. In any data restriction, the data controller must inform the data subjects about the restriction, be in the position to prove the necessity of the restriction, and take all the required measures for the protection of data subjects (Art 10 and 11 Greek Law).

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

No Deviation

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

No Deviation

SECURITY OF PROCESSING (ART 32)

No Deviation

DATA BREACH (ART 33 & 34)

VARYING PROVISION: Data breach notification requirements to individuals are waived (combination of Art 23 and Art 34 GDPR) when the breach notification relates to national security; public defense; crime prevention; important economic or financial interests; establishment, exercise, or defense of legal claims; and the protection of the data subject or the rights and freedoms of others. In all these cases, the data controller must notify the supervisory authority, which ultimately decides whether these criteria are met, and therefore notification to data subjects is not required (Art 11 Greek Law).

DATA PROTECTION OFFICER (ART 37(4))

ADDITIONAL REQUIREMENT: In addition to the GDPR requirements, the Greek DPA will issue a list with examples of controllers it deems should appoint a DPO. The courts are not required to appoint a DPO (Art 14 Greek Law).

DATA TRANSFER DEROGATIONS (ART 49(5))

No Deviation

POWERS SUPERVISORY AUTHORITIES (ART 58)

VARYING PROVISION: Apart from the Article 58 powers, the Greek DPA can conduct investigations without warning, or pursuant to a complaint, to explore compliance with the GDPR. The Greek DPA can access any information it deems fit during an investigation, and no confidentiality provisions can overrule such power. Every public authority is also required to assist the DPA in its investigation. The DPA can issue cautions, instruct the data controller to rectify its data processing activities within a deadline, or restrict processing fully or partially. It can also announce its investigations to the Greek parliament or judicial authorities (Art 62 Greek Law).

CLASS ACTIONS (ART 80 (2))

No Deviation

ADMINISTRATIVE SANCTIONS (ART 83)

SPECIFYING PROVISIONS: The Greek Law clarifies the nature of the administrative sanctions, the process to appeal those sanctions through the highest court of appeal ("Symvoulio Epikrateias"), and which authority is enshrined with fine collection (Arts 67–69 Greek Law).

PENALTIES (ART 84)

SPECIFYING PROVISIONS: The following criminal penalties are foreseen:

Imprisonment for an intentional data breach.

Imprisonment of at least 1 year, and a personal fine of €10,000–100,000, for an intentional data breach that involves sensitive data.

Imprisonment of at least 3 years, and a personal fine of €100,000–300,000, for an intentional data breach that aims to financial profit.

Imprisonment of at least 5 years, and a personal fine of €100,000–300,000, for an intentional data breach that endangers public safety or the constitutional order.

Imprisonment of at least 1 year, and a personal fine of €10,000–100,000, for a DPO who breaches their confidentiality obligations (Art 70 Greek Law).

HR PROCESSING (ART 88)

No Deviation

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

No Deviation

OBLIGATIONS OF SECRECY (ART 90)

No Deviation

LOCAL DPA GUIDANCE & LEGAL SOURCES

Νόμος για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα (Greek Data Protection Act)

IRELAND

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME
Ireland

STATUS: ADOPTED

LAWFULNESS OF PROCESSING (ART 6)

✓

SPECIFYING REQUIREMENT: Communication with data subjects by political parties and candidates for and holders of certain elective offices are considered to be the performance of a task carried out in the public interest (Art 39 Irish Act) (Art 6(1)(e) GDPR).

CHILD'S CONSENT (ART 8)

✓

SPECIFYING REQUIREMENT:

1. **Age:** The age of a child is 16 years old (Art 31 Irish Act) (Art 8(1) GDPR).
2. **Scope:** Information society services do not include preventative or counseling services (Art 31 Irish Act) (Art 8(1) GDPR).

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

✓

ADDITIONAL REQUIREMENT:

1. **Processing for insurance and pension purposes:** Data concerning health may be processed for the purposes of (1) a policy of insurance or life assurance; (2) a policy of health insurance or health-related insurance; (3) an occupational pension, a retirement annuity contract, or any other pension arrangement; or (4) the mortgaging of property (Art 50 Irish Act) (Art 9 GDPR).

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

✓

ADDITIONAL REQUIREMENT: The Irish Act permits processing of personal data relating to criminal convictions and offenses where:

1. **Under the control of official authority:** Processing is permitted under the control of the official authority (1) for the administration of justice; (2) in the exercise of a regulatory, authorizing, licensing function or in determining the eligibility for benefits or services; (3) to protect 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 authorized to carry on a profession or other activity; (4) for enforcement actions aimed at the prevention, detection, or investigation of national or EU law breaches subject to civil or administrative sanctions; (5) for archiving in the public interest, scientific or historical research purposes, or statistical purposes when carried out in accordance with Section 42 of the Irish Act.

2. **Consent:** The data subject gives explicit consent for specific purposes, except where EU or national law prohibits the processing.
3. **Legal claims:** Processing is necessary for providing or obtaining legal advice or in connection with actual or prospective legal claims and proceedings, or is otherwise necessary for the establishment, exercise, or defense of legal rights.
4. **Prevention of injury or damage:** Processing is necessary to prevent injury or other damage to an individual or loss of, or damage to, property or otherwise to protect the vital interests or property of an individual.
5. **Pursuant to national regulations:** Regulations may be made to permit processing if necessary for risk assessment of fraud or fraud prevention, risk assessment of bribery or corruption, or both; or to prevent bribery or corruption, or both; or to ensure network and information systems security and to prevent attacks on and damage to computer and electronic communications services (Art 55 Irish Act) (Art 10 GDPR).

AUTOMATED INDIVIDUAL DECISION MAKING (ART 22)

ADDITIONAL REQUIREMENT: In addition to the exceptions in the GDPR, the right of the individual not to be subject to automated decision making shall not apply when the decision is authorized or required by an enactment and either (1) the effect of that decision is to grant a request of the individual; or (2) if (1) is not applicable, the controller ensures measures are taken to safeguard the individual's legitimate interests (in some instances, the controller is under additional obligations to comply with a request and to notify the individual of certain information) (Art 57 Irish Act) (Art 22 GDPR).

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

ADDITIONAL REQUIREMENT:

1. Restrictions of data subject rights: An individual's rights are restricted to the extent that:

   (1) The restrictions are necessary for:

   a. Safeguarding cabinet confidentiality, parliamentary privilege, national security, defense, and international relations.

   b. Prevention, detection, investigation, and prosecution of criminal offenses and the execution of criminal penalties.

   c. Administration of taxes, duties, or other money due or owing to the state or other public authority or body.

   d. Establishment, exercise, or defense of an actual or prospective legal claim or proceeding.

   e. Administration of any tax, duty, or other money due or owed to the government in any case in which the non-application of the relevant restrictions would be likely to prejudice the aforementioned administration.

   f. Establishment, exercise, or defense of an actual or prospective legal claim or proceeding.

   g. Enforcement of civil law claims.

   h. Estimating the liability of a controller on foot of a claim where application of rights or obligations would likely prejudice the commercial interests of the controller.

   (2) Personal data relating to the data subject is an expression of opinion given in confidence or on the understanding it would be treated as confidential.

   (3) The personal data concerned is kept by the Data Protection Commission, Information Commissioner, or the Comptroller and Auditor General for performance of their functions.

2. **Potential regulatory restrictions for physical or mental health:** An individual's rights may be restricted by means of regulation by the minister when considered necessary for the protection of individuals' rights and freedoms: (1) if the application of those rights would be likely to cause serious harm to the physical or mental health of the data subject and to the extent to which, and for as long as, such application would be likely to cause such harm; and (2) in relation to personal data kept for or related to the social work of a public authority or other body.
3. **Potential regulatory restrictions for the public interest:** An individual's rights may be restricted by means of regulations made by a relevant minister in order to safeguard important objectives of general public interest. Objectives of general public interest include: (1) prevention of threats to public security and safety; (2) avoiding obstructions to justice (legal proceedings and investigation); (3) preventing, detecting, investigating, and prosecuting breaches of discipline by, or the unfitness or incompetence of, regulated professionals and for imposing related sanctions; (4) preventing, detecting, investigating, and prosecuting breaches of ethics for regulated professions; (5) taking any action for considering and investigating complaints made to a regulatory body about a person engaged in a professional or other regulated activity; (6) preventing, detecting,

investigating, and prosecuting civil or administrative infringements and executing related sanctions; (7) identifying assets obtained through criminal conduct and for investigating, taking appropriate action, or the like in any related proceedings; (8) ensuring the effective operations of immigration systems, international protection systems, and the systems for acquisition by persons of Irish citizenship, including by preventing, detecting, and investigating abuses of those systems or related infringements; (9) safeguarding the economic or financial interests of the EU or state; (10) safeguarding monetary policy, the smooth operation of payments systems and deposit-guarantee schemes, effective regulation of financial service providers, and consumer protection; (11) protecting the public against financial loss or detriment; (12) protecting public health and safety and protecting the public against discrimination or unfair treatment in the provision of goods and services; (13) maintaining registers in the public interest; (14) safeguarding the integrity and security of examination systems; and (15) safeguarding public health, social security, social protection, and humanitarian activities (Art 60 Irish Act) (Art 23 GDPR).

4. Right of access: The right of access to a result or script of an exanimation or to the result of an appeal is considered to be made at the later of the date of first publication of the results of the examination or appeal, or the date of the request (Art 56 Irish Act) (Art 23 GDPR).
5. Right to object: The right to object shall not apply to processing, including direct mailing, for election purposes and by the Referendum Commission (Arts 58, 59 Irish Act) (Art 23 GDPR).
6. Legal proceedings: Individuals' rights are restricted to the extent that the restrictions are necessary and proportionate to safeguard judicial independence and court proceedings (Art 158 Irish Act) (Art 23 GDPR).
7. Legal privilege: Individuals' rights do not apply to personal data related to legal advice or legal privilege and when the exercise of such rights would constitute a contempt of court (Art 162 Irish Act) (Art 23 GDPR).

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

✗

No Deviation

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

✗

No Deviation

SECURITY OF PROCESSING (ART 32)

✗

No Deviation

DATA BREACH (ART 33 & 34)

✗

No Deviation

DATA PROTECTION OFFICER (ART 37(4))

✓

SPECIFYING REQUIREMENT: Potential regulations: The minister may issue regulations for the designation of a data protection officer (Art 34 Irish Act) (Art 37(4) GDPR).

CERTIFICATION (ART 42)

✓

SPECIFYING PROVISION: The Irish National Accreditation Board is the accreditation body for the purposes of Art 43(1) GDPR (Art 35 Irish Act) (Art 42 & 43 GDPR).

DATA TRANSFER DEROGATIONS (ART 49(5))

✗

No Deviation

POWERS SUPERVISORY AUTHORITIES (ART 58)

✓

ADDITIONAL REQUIREMENT: The SA can appoint "authorized officers" at its own discretion who can exercise powers under Section 130 of the Irish Act. These powers are broadly similar to those of inspectors appointed under other legislation of this kind.

In cases of urgency to protect individuals' rights and freedoms, the SA may apply in a summary manner, on notice to the controller or processor, to the High Court for an order suspending, restricting, or prohibiting data processing or transfer of data to a third country or international organization (Art 129, 130, 134 Irish Act) (Art 58 GDPR).

CLASS ACTIONS (ART 80 (2))

✗

No Deviation

ADMINISTRATIVE SANCTIONS (ART 83)

✓

ADDITIONAL REQUIREMENT: Administrative fines apply to (1) offenses involving the processing of a child's (here, age 18 or younger) data for direct marketing, profiling, or microtargeting; (2) the exercise of the SA's corrective power; and (3) failures to comply with an enforcement notice (Art 30, 115, 133 Irish Act) (Art 83 GDPR).

When the DPA decides to impose fines on a public authority or body that is not considered an undertaking under the Irish Competition Act 2002, the maximum fine is €1 million (Art 141 Irish Act) (Art 83 GDPR). In addition, the DPA cannot impose administrative fines if the controller/processor has already had criminal law sanctions imposed upon it (Art 136 Irish Act).

PENALTIES (ART 84)

✓

SPECIFYING REQUIREMENT: Offenses related to the unauthorized disclosure by a processor or the disclosure of personal data obtained without authority are subject to a fine and/or imprisonment. The SA may bring and prosecute summary proceedings for any such offenses (Art 144–147 Irish Act) (Art 84 GDPR).

HR PROCESSING (ART 88)

✓

ADDITIONAL REQUIREMENT: The practice of "enforced data subject access" (requiring an individual to make a subject access request or to supply information obtained from a subject access request) is prohibited in the employment context (Art 4 Irish Act) (Art 88 GDPR).

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

✓

ADDITIONAL REQUIREMENT: The individual right to access, correction, restriction, objection, and data portability are restricted when processing is carried out for archiving in the public interest, scientific or historical research, or statistical purposes insofar as the exercise of these rights: (1) would likely render impossible, or seriously impair, the achievement of those purposes; and (2) such restriction is necessary for the fulfillment of those purposes.

When data is processed for these purposes and another purpose at the same time, these restrictions apply only to the extent the processing relates to those purposes (Art 61 Irish Act) (Art 23 GDPR).

OBLIGATIONS OF SECRECY (ART 90)

✗

No Deviation

LOCAL DPA GUIDANCE & LEGAL SOURCES

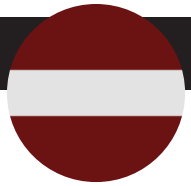
✓

Data Protection Act 2018

REMARKS

✓

The Irish Act restructured the Office of the Data Protection Commissioner as the Data Protection Commission, which will be headed by up to three commissioners appointed for terms of 4–5 years. When there is more than one commissioner, the Minister of Justice will appoint a chairperson, who shall have the tiebreaking vote among the commissioners.



LATVIA

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Likumprojekts "Personas datu apstrādes likums"

STATUS: DRAFT

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

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 Deviation

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 Deviation

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;

(1) antidiscrimination; (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 Deviation

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

✗

No Deviation

SECURITY OF PROCESSING (ART 32)

✗

No Deviation

DATA BREACH (ART 33 & 34)

✗

No Deviation

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 Deviation

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 Deviation

ADMINISTRATIVE SANCTIONS (ART 83)

✗

No Deviation

PENALTIES (ART 84)

✗

No Deviation

HR PROCESSING (ART 88)

✗

No Deviation

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

✗

No Deviation

OBLIGATIONS OF SECRECY (ART 90)

✗

No Deviation

LOCAL DPA GUIDANCE & LEGAL SOURCES

✓

Likumprojekts "Personas datu apstrādes likums"

LUXEMBOURG

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et 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 (règlement général sur la protection des données), portant modification du Code du travail et de la loi modifiée du 25 mars 2015 fixant le régime des traitements et les conditions et modalités d'avancement des fonctionnaires de l'État.

STATUS: ADOPTED

SME EXCEPTION

✗

No Deviation

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

CHILD'S CONSENT (ART 8)

✗

No Deviation

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

✓

VARYING:

Prohibition of processing genetic or biometric data for life insurance or medical insurance purposes.

CCTV (ART 6)

✗

No Deviation

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

✓

SPECIFYING:

Employers can ask future employees to provide an extract of their criminal record in the recruitment process. The employer can use the extract only for recruitment purposes or human resources purposes and cannot be kept for more than one month.

INFORMATION OBLIGATION (ART 13 & 14)

✓

SPECIFYING:

Information obligations are applicable to the extent they do not violate the freedom of expression, freedom of journalism, or literary expression.

AUTOMATED INDIVIDUAL DECISION MAKING (ART 22)

✗

No Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

✗

No Deviation

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

✗

No Deviation

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

✗

No Deviation

SECURITY OF PROCESSING (ART 32)

✗

No Deviation

DATA BREACH (ART 33 & 34)

✗

No Deviation

DATA PROTECTION IMPACT ASSESSMENT (ART 35)

✓

VARYING:

The CNPD has the authority to draw a list of "high-risk processing" that requires a DPIA but has not done so yet.

DATA PROTECTION OFFICER (ART 37(4))

✗

No Deviation

CERTIFICATION (ART 42)

✗

No Deviation

DATA TRANSFER DEROGATIONS (ART 49(5))

✗

No Deviation

POWERS OF SUPERVISORY AUTHORITIES (ART 58)

✓

ADDITIONAL:

The SA is appointed to a five-year term.

CLASS ACTIONS (ART 80(2))

✓

SPECIFYING:

The CNPD can intervene and examine a case pursuant to an application made under Article 80 of the GDPR.

ADMINISTRATIVE SANCTIONS (ART 83)

✓

SPECIFYING:

The CNPD may also impose penalties amounting to up to 5% of a company's average daily turnover achieved during the previous financial year to motivate a company to provide requested information or if a company is not cooperating.

PENALTIES (ART 84)

SPECIFYING:

Anybody who intentionally prevents or obstructs the performance of the CNPD's duties may be subject to: (1) a prison sentence of between eight days and one year; and/or (2) a fine of €251–125,000.

FREEDOM OF EXPRESSION AND INFORMATION (ART 85)

No Deviation

HR PROCESSING (ART 88)

No Deviation

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

No Deviation

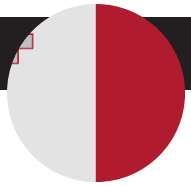
OBLIGATIONS OF SECRECY (ART 90)

VARYING:

Secrecy does not apply to communication with an attorney, notary public, or accountant or otherwise an activity covered by professional secrecy.

LOCAL DPA GUIDANCE AND LEGAL SOURCES

Act establishing the National Commission for Data Protection and implementing Regulation (EU) 2016/679 on the protection of individuals with regard to the protection of personal data processing of personal data and the free movement of such data, and repealing Directive 95/46 / EC (General Data Protection Regulation), amending the Labor Code and the amended Law of 25 March 2015 laying down the salary system and the conditions and procedures for the advancement of State officials: Law of 1 August 2018 on the organization of the National Commission for Data Protection and the General Scheme on Data Protection



MALTA

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Data Protection Act, Cap. 586 (May 28, 2018) [relevant subsidiary legislations referenced and provided below]

STATUS: ADOPTED

SME EXCEPTION

✗

No Deviation

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

CHILD'S CONSENT (ART 8)

✓

POSSIBLE REGULATIONS:
The minister for data protection may, after consulting with the SA, prescribe regulations for establishing the age for a child's consent to information society services (Art 33(g) Maltese Act) (Art 8 GDPR).

SPECIFYING PROVISION:
The processing of personal data of a child for information society services is lawful when the child is 13 years old (Art 4 Subsidiary Legislation 586.11) (Art 8 GDPR).

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

✓

ADDITIONAL REQUIREMENT:

When a controller intends to process the following personal data in the public interest, the controller must consult with and obtain prior authorization from the SA: (1) genetic data, biometric data, or data concerning health for statistical purposes; (2) genetic data, biometric data, or data concerning health for research purposes (in these instances, the SA must consult a research ethics committee or relevant institution); or (3) special categories of data for the management of social services and systems (Art 7 Maltese Act).

An identity document can only be processed if the national identity number or other identifiers will only be used under appropriate safeguards for individuals' rights and freedoms and when processing is clearly justified, taking into account the purpose of processing and (1) the importance of a secure identification; or (2) any other valid reason permitted by law (Art 8 Maltese Act) (Art 9(4) GDPR).

The processing of data concerning health is lawful when subject to suitable and specific safeguards and when necessary and proportionate for the purposes of an insurance policy and (1) the controller

cannot reasonably be expected to obtain an individual's consent; and (2) the controller is not aware that the data subject is withholding consent (Art 4 Subsidiary Legislation 586.10) (Art 9(4) GDPR).

CCTV (ART 6)

No Deviation

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

No Deviation

INFORMATION OBLIGATION (ART 13 & 14)

No Deviation

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

No Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

RESTRICTING REGULATIONS:

The minister may restrict individuals' rights by means of regulation (Art 5 Maltese Act) (Art 23 GDPR).

Any restriction to individuals' rights must respect individuals' fundamental rights and freedoms and must be a necessary and proportionate measure. A restriction will only apply when necessary for: (1) safeguarding and maintaining national security, public security, defense, and international relations; (2) preventing, detecting, investigating, and prosecuting criminal offenses and the execution of related penalties; (3) administering tax, duty, fines, fees, or other money due or owed to the state; (4) administering social security benefits and when such data has been obtained in confidence when carrying out an investigation against fraud; (5) establishing, exercising, or defending legal claims; (6) performing functions of the SA; (7) delivering social services by a public authority or other body in instances when data was obtained in confidence for the purposes of delivering such services; (8) health data when it would be likely that the exercise of rights would cause serious harm to the vital interests of a patient; and (9) matters relating to Maltese citizenship when the relevant minister or authorized person refuses an application for citizenship (Art 4 & 7 Subsidiary Legislation 586.09).

The retention period for personal data subject to a restriction should not be longer than: (1) what is necessary for the purposes of processing; (2) the period required to achieve the aim of the restriction; or (3) as permitted by law (Art 5 Subsidiary Legislation 586.09).

The controller must inform the data subject about any restriction, provided such disclosure will not be prejudicial to the purposes of the restriction (Art 6 Subsidiary Legislation 586.09) (Art 23 GDPR).

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

No Deviation

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

No Deviation

SECURITY OF PROCESSING (ART 32)

No Deviation

DATA BREACH (ART 33 & 34)

No Deviation

DATA PROTECTION IMPACT ASSESSMENT (ART 35)

No Deviation

DATA PROTECTION OFFICER (ART 37(4))

POSSIBLE REGULATIONS:

The minister may, after consulting with the SA, prescribe regulations for DPO appointments (Art 33 Maltese Act) (Art 37(4) GDPR).

CERTIFICATION (ART 42)

SPECIFYING PROVISION:

The certification body will be accredited by the National Accreditation Board (Malta) (Art 32 Maltese Act) (Art 42 & 43 GDPR).

DATA TRANSFER DEROGATIONS (ART 49(5))

RESTRICTING REGULATIONS:

The minister may, after consulting with the SA, prescribe regulations that set limits on the transfer of specific categories of personal data to a third country or international organization for important reasons of public interest (Art 10 Maltese Act) (Art 49(5) GDPR).

POWERS OF SUPERVISORY AUTHORITIES (ART 58)

SPECIFYING PROVISION:

The SA (1) has the power to institute civil judicial proceedings for violations of the Maltese Act or GDPR; (2) may seek the advice of and consult with any other competent authority in the exercise of the SA's functions; (3) in the exercise of investigative powers, may request the assistance of the executive police to enter and search any premises; and (4) in the event of joint operations with other SAs, may confer powers, including investigative powers, on the secondary SA's staff (Art 15 & 16 Maltese Act).

The SA also has recourse to civil action to recover amounts due when a notice imposing an administrative fine is served and (1) the person fails to appeal within the applicable timeframe and fails to pay the fine; or (2) the person appeals to the tribunal and the appeal is withdrawn or the tribunal determines the appropriate fine and no further appeal is filed with the Court of Appeal, or if an appeal is filed with the Court of Appeal and the court determines the appropriate penalty, or the imposed penalty is not paid within 15 days from the date of the decision or the withdrawal of the appeal, or the date when the tribunal or the Court of Appeal determines the appropriate fine or penalty (Art 20(3) Maltese Act)) (Art 58 GDPR).

CLASS ACTIONS (ART 80(2))

No Deviation

ADMINISTRATIVE SANCTIONS (ART 83)

SPECIFYING PROVISION:

The SA may impose an administrative fine on a public authority or body: (1) of up to €25,000 per violation of Art 83(4) GDPR, and, additionally, a daily fine of €25 for each day the violation persists; and (2) of up to €50,000 per violation of Art 83(5, 6) GDPR and, additionally, a daily fine of €50 for each day the violation persists (Art 21 Maltese Act) (Art 83 GDPR).

The Act establishes the Information and Data Protection Appeals Tribunal, which consists of a chairperson and two other members appointed by the minister, and has the same powers as the First Hall, Civil Court. Individuals have a right to appeal, on certain grounds, to the tribunal when the SA has made a legally binding decision and to the Court of Appeal (Art 24, 26, 27 & 29 Maltese Act) (Art 83 GDPR).

POSSIBLE REGULATIONS:

The minister may, after consulting with the SA, prescribe regulations for fees that may be levied by the SA (Art 33 Maltese Act) (Art 83 GDPR).

PENALTIES (ART 84)

SPECIFYING PROVISION:

Any person who knowingly provides false information to the SA pursuant to his/her investigative powers or does not comply with any lawful request by the SA in the course of an investigation is in violation of the Act, punishable by fine (€1,250 to €50,000) and/or imprisonment (up to 6 months). The SA must provide information to any officer of the Executive Police before initiating proceedings for such alleged infringements (Art 22 Maltese Act) (Art 84 GDPR).

POSSIBLE REGULATIONS:

The minister may, after consulting with the SA, prescribe regulations for criminal penalties imposed under the Act (Art 33 Maltese Act) (Art 84 GDPR).

FREEDOM OF EXPRESSION AND INFORMATION (ART 85)

SPECIFYING PROVISION:

Personal data processing for the purpose of exercising the right to freedom of expression and information is exempted or derogated from the following GDPR provisions: (1) principles related to processing, Art 5(1)(a–e) GDPR; (2) lawfulness of processing, Art 6 GDPR; (3) conditions for consent, Art 7 GDPR; (4) processing relating to criminal convictions and offenses, Art 10 GDPR; (5) processing not requiring identification, Art 11(2) GDPR; (6) information provided to data subjects, Art 13(1–3) & 14(1–4) GDPR; (7) right of access, Art 15(1–3) GDPR; (8) right to erase, Art 17(1–2) GDPR; (9) right to restriction, Art 18(1)(a, b, d) GDPR; (10) right to data portability, Art 20(1–2) GDPR; (11) right to object, Art 21(1) GDPR; (12) data protection by design and default, Art 25 GDPR; (13) representatives of controllers or processors not established in the EU, Art 27 GDPR; (14) records of processing, Art 30 GDPR; (15) data breach notification, Art 33 & 34 GDPR; (16) certification and certification bodies, Art 42 & 43 GDPR; (17) cooperation, Art 60–62 GDPR; and (18) consistency, Art 63–67 GDPR (Art 9 Maltese Act) (Art 85 GDPR).

HR PROCESSING (ART 88)

No Deviation

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

SPECIFYING PROVISION:

"Statistical purposes" is further articulated under the definition "official statistics," which is information collected, analyzed, and produced for the benefit of society to characterize collective phenomena in a considered population and produced by the Maltese National Statistics Office as provided for by law, or by other national authorities as designated by Eurostat following recommendation by the National Statistics Office (Art 3 Maltese Act) (Art 89 GDPR).

See also Art 6 Maltese Act.

OBLIGATIONS OF SECRECY (ART 90)

No Deviation

LOCAL DPA GUIDANCE AND LEGAL SOURCES

Data Protection Act (in English)

Restriction of the Data Protection (Obligations and Rights) Regulations [Subsidiary Legislation 586.09] (in English)

Processing of Data Concerning Health for Insurance Purposes Regulations [Subsidiary Legislation 586.10] (in English)

Processing of Child's Personal Data in Relation to the Offer of Information Society Services Regulations [Subsidiary Legislation 586.11] (in English)

REMARKS

The Maltese Act establishes the office of the SA, or the Information and Data Protection Commissioner, who may hold office for a term of five years with the possibility of reappointment (Art 11 & 14 Maltese Act) (Art 51–57 GDPR).

Actions taken against a controller and/or processor that are filed with the First Hall, Civil Court, per Art 30 of the Maltese Act, must be commenced within 12 months from the date when the individual became or ought to have reasonably become aware of an alleged infringement (Art 30 Maltese Act) (Art 82 GDPR).

THE NETHERLANDS

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Wet van 16 mei 2018, houdende regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming)

STATUS: ADOPTED

SME EXCEPTION

✗

No Deviation

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

CHILD'S CONSENT (ART 8)

✓

SPECIFYING REQUIREMENT:

1. **Age:** A user must be at least 16 years old to consent to information society services directed at children (Art 5(1) Dutch Act).

2. **Individual Rights:** The person holding parental responsibility shall exercise individual rights on behalf of someone less than 16 years old (Art 5(4) Dutch Act).

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

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

✓

DEVIATING REQUIREMENT:

1. **Genetic Data:** 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 (Art 28 Dutch Act).

2. **Biometric Data:** The prohibition to process biometric data does not apply when this occurs for security or authentication purposes (Art 29 Dutch Act).

3. Health Data: The prohibition to process health data does not apply to (Art 30 Dutch Act):

(a) Administrative bodies, pension funds, employers, or institutions acting on their behalf, provided processing is carried out to comply with a legal obligation (e.g., pension laws) or for the reintegration or assistance of employees or (unemployed) beneficiaries connected to sickness or disability.

(b) Schools, to the extent processing is necessary for assistance of scholars or to take special measures with regard to their health condition.

(c) Specific institutions (rehabilitation institutions, the Justice Department in the context of a prison sentence, institutions in the context of certain social security matters).

(d) Care providers, to the extent necessary to ensure treatment of the data subject, or the administration/ management of an institution or medical practice. Also note that any other additional sensitive data can be processed by this category if necessary for adequate medical treatment of the data subject.

(e) Insurance companies, to the extent necessary to assess the risk that must be insured or for the execution of the insurance agreement.

Note that all of the above categories of processors of health data must be bound to or respect confidentiality.

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

DEVIATING REQUIREMENT:

Criminal Data Processing: Except for what is set forth in Article 10 GDPR, criminal convictions and related security measure data may be processed in the following specific cases: (1) the individual provided explicit consent; (2) processing 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 rendered the data public himself; (4) processing is necessary in light of litigation; (5) processing is necessary for reasons of predominant public interest; (6) 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 make a decision about him; and (9) processing is carried out by controllers operating under a specific license (Art 31–33 Dutch Act). When these legislative provisions or Article 10 GDPR is violated, the authority is competent to impose the maximum fine of 4% of worldwide turnover or €20 million, whichever is higher (Art 17 Dutch Act).

INFORMATION OBLIGATION (ART 13 & 14)

No Deviation

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

DEVIATING REQUIREMENT: The prohibition on automated individual decision making does not apply when that decision making, other than profiling, is necessary to comply with a legal obligation imposed to the controller or for the performance of a task in the public interest (Art 40 Dutch Act).

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

DEVIATING REQUIREMENT:

Restrictions: If there is a data breach, the controller may restrict the data subject's rights and the obligation to notify the data subject to the extent necessary for: (1) national security; (2) national 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 civil monetary claims. When relying on restrictions, the controller still takes account of certain principles, such as the categories of data involved and the measures taken to ensure safe data transfers (Art 41Dutch Act).

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

No Deviation

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

No Deviation

SECURITY OF PROCESSING (ART 32)

No Deviation

DATA BREACH (ART 33 & 34)

VARYING REQUIREMENT:

1. Restrictions to Data Subject's Rights: If there is a data breach, the controller may restrict the data subject's rights and the obligation to notify the data subject to the extent necessary for: (1) national security; (2) national 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 civil monetary claims. When relying on restrictions, the controller still takes account of certain principles, such as the categories of data involved and the measures taken to ensure safe data transfers.

2. Individual Notification Exemption: Undertakings offering financial services (as defined by the Act on Financial Supervision (Wet op Financieel Toezicht)) are not under the obligation to notify the data subject of a data breach (Art 42 Dutch Act).

DATA PROTECTION IMPACT ASSESSMENT (ART 35)

No Deviation

DATA PROTECTION OFFICER (ART 37(4))

No Deviation

CERTIFICATION (ART 42)

No Deviation

DATA TRANSFER DEROGATIONS (ART 49(5))

No Deviation

POWERS SUPERVISORY AUTHORITIES (ART 58)

DEVIATING REQUIREMENT:

1. "Last onder Bestuursdwang": The supervisory authority is competent to impose a last onder bestuursdwang for any violation of the GDPR or the Dutch Act. The last onder bestuursdwang involves remedial action to undo the damage caused by the violation (Art 16 Dutch Act).

2. Act Against EU Decision on Transfers: In the context of an investigation of data transfers initiated by an interested party, the Dutch supervisory authority is competent to act against an adequacy decision or a decision establishing standard contractual clauses taken by the European Commission by filing a request with the Council of State.

3. Dispute Resolution by the Dutch SA: After initiation of court proceedings, the data subject can request the Dutch supervisory authority to assist in mediation of the dispute with the data controller (Art 36 Dutch Act).

CLASS ACTIONS (ART 80 (2))

DEVIATING REQUIREMENT:

Objection Right of Defendant: Class actions in civil and administrative proceedings are only allowed if the defendant does not object (Art 37 Dutch Act).

ADMINISTRATIVE SANCTIONS (ART 83)

SPECIFYING REQUIREMENT:

1. Suspensive Effect of Appeal: An administrative fine is only executable after the appeal or objection term has passed, or if an appeal or objection was filed, after an appeal or objection decision is issued (Art 38 Dutch Act).

2. Administrative Fine on Administrative Official Authorities: The Dutch supervisory authority may impose administrative fines on Dutch administrative official authorities in the same way as it would be imposed on private companies (Art 18 Dutch Act).

PENALTIES (ART 84)

No Deviation

FREEDOM OF EXPRESSION AND INFORMATION (ART 85)

✗

HR PROCESSING (ART 88)

✗

No Deviation

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

✓

DEVIATING REQUIREMENT:

Sensitive Data Processing for Research: The prohibition to process sensitive data does not apply when it is necessary for scientific, research, or statistical purposes and the research is in the public interest; requesting consent places an unreasonable burden or effort; and the data subject's right to privacy is sufficiently safeguarded.

OBLIGATIONS OF SECRECY (ART 90)

✓

DEVIATING REQUIREMENT:

Obligation of Secrecy: The obligation of secrecy or confidentiality imposed on the data protection officer under the GDPR can be lifted by the data subject (Art 39 GDPR).

LOCAL DPA GUIDANCE & LEGAL SOURCES

✓

Dutch Act on the Protection of Personal Data

Dutch SA Guidance on Dutch Act

Dutch SA Guidelines GDPR and Implementing Act

POLAND

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

STATUS: ADOPTED

SME EXCEPTION

✗

No Deviation

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

CCTV

✓

ADDITIONAL REQUIREMENT:

1. Employee CCTV Monitoring:

(a) General Scope and Purposes: The Polish Act modifies the Polish Labor Code in terms of employee monitoring through CCTV and sets forth that this is legitimate when this is done for security purposes (to protect company premises or confidential information) (Art 111 Polish Act).

(b) Exception: CCTV recording may not cover sanitary rooms, cloak rooms, company lunch rooms, and smoking areas unless under specific safeguards (the employees recorded must be unrecognizable).

(c) Retention Period: The CCTV recordings shall be processed solely for security purposes and not stored for a period exceeding three months, except when recordings are used in judicial proceedings. In such case, recordings may be kept until the end of such proceedings.

(d) Notice: The employer is required to provide notice to the employees about CCTV monitoring, except when it is covered by a collective labor agreement (in which case notice may be given there). Notice must be given no later than one day before the launch of CCTV monitoring and may be done in the form of appropriate signage or sound notices indicating which area is being monitored.

2. CCTV Monitoring in Public Places:

(a) General Scope and Purposes: Municipalities may install CCTV monitoring for security purposes in public areas (including in and around public buildings) (Art 114 Polish Act).

(b) Exception: CCTV recording may not cover sanitary rooms, cloak rooms, company lunch rooms, social facilities, and smoking areas.

(c) Retention Period: The CCTV recordings shall be processed solely for security purposes and not stored for a period exceeding three months, except when recordings are stored on explicit legal basis.

(d) Notice: Notice shall be provided by appropriate signage.

EMPLOYEE EMAIL MONITORING

✓

ADDITIONAL REQUIREMENT:

General Scope and Purposes: An employer may conduct email monitoring of its employees to the extent this is necessary to verify work performance and proper use of company IT devices (Art 111 Polish Act). Email monitoring cannot violate the secrecy of correspondence.

CHILD'S CONSENT (ART 8)

✗

No Deviation

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

✗

No Deviation

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

✗

No Deviation

INFORMATION OBLIGATION (ART 13 & 14)

✗

No Deviation

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

✗

No Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

✓

DEVIATING REQUIREMENT:

Right of Access and Information: The data controller that is exercising a task in the public interest does not need to disclose information regarding further processing purposes when this is necessary to comply with the task of public interest or when this is necessary to protect confidential information (Art 3 Polish Act).

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

✗

No Deviation

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

✗

No Deviation

SECURITY OF PROCESSING (ART 32)

✗

No Deviation

DATA BREACH (ART 33 & 34)

✗

No Deviation

DATA PROTECTION IMPACT ASSESSMENTS (ART 35)

✗

No Deviation

DATA PROTECTION OFFICER (ART 37(4))

✓

SPECIFYING REQUIREMENT:

1. Definition of "Public Authority": "Public authorities" required to appoint a DPO are defined as units of the public finance sector, research institutes, and the National Bank of Poland (Art 9 Polish Act).

2. Notification Procedure: The appointed DPO, with relevant contact details, must be announced (in electronic form) to the Polish supervisory authority within 14 days following appointment. In the same manner, the data controller must notify the SA within 14 days of any change in appointment of the DPO (Art 10 Polish Act).

CERTIFICATION (ART 42)

SPECIFYING REQUIREMENT:

1. Application for Certification: Applications for certification must contain at least the contact details of the entity wishing to apply for certification, motivation of compliance with certification criteria, and indication of the scope of the requested certification (Art 17 Polish Act). The SA must examine the application within three months after submission of the application (Art 18 Polish Act).

2. Inspection: The SA is competent to carry out inspection activities to verify compliance with a granted certificate (Art 24–25 Polish Act).

DATA TRANSFER DEROGATIONS (ART 49(5))

No Deviation

POWERS SUPERVISORY AUTHORITIES (ART 58)

SPECIFYING REQUIREMENT:

1. Procedure: The procedure before the Polish supervisory authority is considered an administrative procedure that only accommodates first-instance proceedings (no appeal procedure shall be held before the SA). Appeal against a decision of the supervisory authority must be filed with the competent administrative courts. A translation into Polish may be requested from the applicant (Art 7 and 63 Polish Act).

2. Restrictions on Processing: The SA may restrict a processing activity if it is probable that the processing concerned is a violation of the Polish Act and a restriction is necessary to prevent further harm during proceedings preceding a decision on a potential violation. A restriction may only be imposed to the extent necessary and must allow an acceptable level of processing. A restriction must be limited in time and must end at the latest at the date a decision is taken on a potential violation (Art 70 Polish Act).

3. Preliminary Question to the Polish Administrative Court: If, during proceedings before the supervisory authority, the SA determines that there are reasonable doubts about one of the following decisions of the EU Commission, it can decide to file a request with the Polish Administrative Courts for clarification: (1) decisions on (approved) codes of conduct; (2) adequacy decisions (granting or withdrawals); and (3) standard contractual clauses (Art 71 Polish Act).

4. Cooperation with Other SAs: The Polish SA may impose a provisional penalty if there is a lack of (timely) cooperation from another SA. When doing so, it shall determine the term during which such measure is valid (Art 75 Polish Act).

5. Audits:

(a) Audits: Audits/inspections may be carried out from 6AM to 10PM each day. Auditors may be assisted by experts or by police force when necessary (Art 84–85 Polish Act).

(b) Exclusion for Auditors: Specific members of the SA conducting investigations or audits in the preparation of regulatory proceedings may be excluded if they cannot be considered impartial, for instance if audits can result in benefits to him/her or to his/her spouse, cohabitants, and persons related to the auditor in the second or third degree (Art 80 Polish Act). Any audits/inspections must be carried out upon presentation of a personal authorization document along with a service card and/or a document confirming the auditor's identity. The personal authorization document confirms the legal basis for inspection, the scope of inspection, and the identity of the auditor (Art 81 Polish Act).

CLASS ACTIONS (ART 80 (2))

No Deviation

CIVIL LIABILITY (ART 82)

DEVIATING REQUIREMENT:

Proceedings: When administrative proceedings are pending and civil proceedings are initiated, the civil court shall stay civil proceedings to the extent administrative proceedings were already initiated before the start of civil proceedings (Art 95 Polish Act). A final decision issued by the SA in administrative proceedings is binding upon the court ruling in civil proceedings (Art 97 Polish Act).

ADMINISTRATIVE SANCTIONS (ART 83)

ADDITIONAL REQUIREMENT:

1. Conversion to PLN: The equivalent of the amounts expressed in EUR shall apply converted into PLN based on the average EUR exchange rate as set forth by the National Bank of Poland (Art 103 Polish Act).

2. Specific Maximum Fine for Public Bodies: The following three public bodies are excluded from the maximum administrative fines set forth by the GDPR and can solely be subject to a maximum fine of 100,000 PLN: (1) the public finance sector; (2) research institutes; and (3) the National Bank of Poland (Art 102 Polish Act).

3. Deadline: An administrative fine is payable within 14 days from the day of the administrative decision (Art 105 Polish Act). After this deadline, interest may apply.

PENALTIES (ART 84)

DEVIATING REQUIREMENT:

Imprisonment: The Polish Act imposes imprisonment of up to two years as alternative penalties to the administrative fine (with maximum imprisonment of up to three years if the processing activity involves sensitive data) (Art 107 Polish Act).

FREEDOM OF EXPRESSION AND INFORMATION (ART 85)

No Deviation

HR PROCESSING (ART 88)

No Deviation

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

No Deviation

OBLIGATIONS OF SECRECY (ART 90)

ADDITIONAL REQUIREMENT:

1. Members of the Supervisory Authority: The president, the deputy president, and other members of the SA are bound to confidentiality of all information disclosed to them in the performance of their official duties (Art 46 Polish Act). This confidentiality obligation continues after termination of employment with the SA.
2. Procedure: Documents covered by trade secrets may be filed in redacted from with the supervisory authority in the context of proceedings before the SA. The company must also submit the documents concerned in nonredacted format; however, redaction shall be respected when documents are solicited by other SAs or other official bodies (Art 65 Polish Act).

LOCAL DPA GUIDANCE & LEGAL SOURCES

Polish Act on the Protection of Personal Data

SLOVAKIA

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Zákon o ochrane osobných údajov a o zmene a doplnení niektorých zákonov

STATUS: ADOPTED

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

CHILD'S CONSENT (ART 8)

✗

No Deviation

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

✓

VARYING/ADDITIONAL REQUIREMENT: Consent to process sensitive data is void if its exclusion precludes a separate regulation. Processing is also permitted when (1) necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or the data subject in the area of labor law, social law insurance, social protection, or public health insurance; and (2) necessary for the purpose of social insurance, social security for police and soldiers, and providing specific social benefits (§ 16 Slovakian Act) (Art 9 GDPR).

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

✗

No Deviation

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

✗

No Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

✓

ADDITIONAL REQUIREMENT: Restrictions of data subjects may be restricted if established to ensure Slovak public policy or economic mobilization (§ 30 Slovakian Act) (Art 23 GDPR).

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

No Deviation

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

No Deviation

SECURITY OF PROCESSING (ART 32)

No Deviation

DATA BREACH (ART 33 & 34)

No Deviation

DATA PROTECTION OFFICER (ART 37(4))

No Deviation

DATA TRANSFER DEROGATIONS (ART 49(5))

No Deviation

POWERS SUPERVISORY AUTHORITIES (ART 58)

ADDITIONAL REQUIREMENT: The DPA is authorized to invite the controller or processor to submit an explanation of suspected breaches of the Act, special regulation, or international law. The subject of the DPA's supervision does not include contractual disputes between the controller/processor and another person if the court and other bodies are competent to hear and decide the dispute. The DPA may also charge an appropriate fee for administrative costs or refuse to act on an application if it is manifestly unfounded, inappropriate, or repetitive (§ 80 Slovakian Act) (Art 58 GDPR).

CLASS ACTIONS (ART 80 (2))

No Deviation

ADMINISTRATIVE SANCTIONS (ART 83)

ADDITIONAL REQUIREMENT: The Slovakian Act empowers the DPA to impose a fine of up to €2,000 on persons who are not the controller or processor for failure to cooperate with the DPA. The DPA may also fine the controller or processor if it fails to ensure adequate conditions for the exercise of DPA controls under Article 94 of the Slovakian Act (§§ 104–106 Slovakian Act (Art 83 GDPR).

PENALTIES (ART 84)

No Deviation

HR PROCESSING (ART 88)

No Deviation

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

No Deviation

OBLIGATIONS OF SECRECY (ART 90)

SPECIFYING REQUIREMENT: The Slovakian Act requires controllers and processors to maintain the confidentiality of personal data even after the processing of that data has ended or after an employment relationship is terminated. This obligation does not apply if it's necessary to perform tasks necessary for judicial or law enforcement proceedings under Slovakian law (§ 79 Slovakian Act) (Art 90 GDPR).

LOCAL DPA GUIDANCE & LEGAL SOURCES

Zakón o ochrane osobných údajov a o zmene a doplnení niektorých zákonov (Slovak Data Protection Act)

SPAIN

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Proyecto de Ley Orgánica de Protección 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 Deviation

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

No Deviation

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 Deviation

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 Deviation

DATA BREACH (ART 33 & 34)

No Deviation

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 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 Deviation

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 Deviation

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 Deviation

HR PROCESSING (ART 88)

No Deviation

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 & 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.

The Spanish government has approved the Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos (BOE, núm. 183, de 30 de julio de 2018) ("Royal Decree-law 5/2018"). This provisional legislation will be in force until the Spanish Act is enacted. The law sets out the following:

- **Chapter I: Investigative Powers:** The SA, or the Spanish Data Protection Agency, has investigative powers including conferring power to seconding SA's staff (Art 58(1) & 62(3) GDPR).
- **Chapter II: Sanctions Regime:** The statute of limitations for infringements of Art 83(4) GDPR and Art 83(5) & (6) GDPR is two years and three years, respectively. The statute of limitations for payment of fines is one year for fines less than €40,000, two years for fines between €40,001 and €300,000, and three years for fines over €300,000 (Art 83 GDPR).
- **Chapter III: Procedures for Violations of Data Protection Regulation:** This chapter details the procedures, such as the type of claims that may be submitted to the SA and determination of territorial scope, for possible violations of the GDPR or Spanish data protection laws (Art 4(23), 55, 56 & 68(4) GDPR).
- **Transitory provision:** Data processing agreements entered into before May 25, 2018, remain in force until their termination date or until May 25, 2022, if there is no termination date. During this period, either party may request to modify the contract to comply with Art 28 GDPR (Art 28 GDPR).

SWEDEN

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Lag Med Kompletterande Bestämmelser Till EU Dataskyddsförordning

STATUS: ADOPTED

SME EXCEPTION

✗

No Deviation

LAWFULNESS OF PROCESSING (ART 6)

✗

No Deviation

CHILD'S CONSENT (ART 8)

✓

SPECIFYING REQUIREMENT:

Age: A user must be at least 13 years old to consent to information society services directed at children (Ch 3 Sec 4 Swedish Act). Sensitive data (genetic, biometric, and health data)

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

✓

DEVIATING REQUIREMENT:

Social Security Number Processing: The processing of social security numbers is permitted without the data subject's consent when this is necessary for security or authentication purposes (Ch 3 Sec 9 Swedish Act).

CRIMINAL CONVICTIONS/SECURITY MEASURES (ART 10)

✓

DEVIATING REQUIREMENT:

1. **Compliance with Local Storage/Archive Requirements:** The processing of criminal data is permitted if it is necessary to comply with storage/archive regulations (Ch 3 Sec 8 Swedish Act).
2. **Maximum Administrative Fine Applicable:** A violation of Art 10 GDPR is subject to the maximum administrative fine set forth in Art 83(5) GDPR (as converted into SEK, see below) (Ch 6 Sec 3 Swedish Act).

INFORMATION OBLIGATION (ART 13 & 14)

No Deviation

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

No Deviation

RESTRICTIONS TO DATA SUBJECT'S RIGHTS (ART 23)

DEVIATING REQUIREMENT:

Right of Access: The data subject's right of access is limited when the data controller is not permitted to disclose the personal data of the data subject on the basis of local law (Ch 5 Sec 1 Swedish Act). In addition, this right is restricted if the personal data is included in a non-finalized document, unless (1) the data is already made publicly available; (2) the data is treated solely for archival purposes in the general interest or statistical purposes; or (3) the document has been in a "non-finalized" state for more than a year (Ch 5 Sec 2 Swedish Act).

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

No Deviation

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

No Deviation

SECURITY OF PROCESSING (ART 32)

No Deviation

DATA BREACH (ART 33 & 34)

No Deviation

DATA PROTECTION IMPACT ASSESSMENT (ART 35)

No Deviation

DATA PROTECTION OFFICER (ART 37(4))

No Deviation

CERTIFICATION (ART 42)

No Deviation

DATA TRANSFER DEROGATIONS (ART 49(5))

No Deviation

POWERS SUPERVISORY AUTHORITIES (ART 58)

No Deviation

CLASS ACTIONS (ART 80 (2))

No Deviation

ADMINISTRATIVE SANCTIONS (ART 83)

SPECIFYING REQUIREMENT:

1. Maximum Administrative Fines Converted into SEK: The maximum administrative fines set forth by the GDPR are converted into SEK as follows:

(a) The cap of €10 million or 2% of annual global turnover included in Art 83(4) GDPR is capped at 5 million SEK (the equivalent of €484,793) by the Swedish Act (Ch 6 Sec 2 Swedish Act).

(b) The cap of €20 million or 4% of annual global turnover included in Art 83(5) and (6) GDPR is capped at 10 million SEK (the equivalent of €968,600) by the Swedish Act (Ch 6 Sec 2 Swedish Act).

2. State Budget: Administrative fines collected go to the state budget (Ch 6 Sec 5 Swedish Act).

3. Collection of Fine Within 30 Days: Administrative fines must be paid within 30 days of the decision issuing the administrative fine (Ch 6 Sec 6 Swedish Act).

PENALTIES (ART 84)

No Deviation

FREEDOM OF EXPRESSION & INFORMATION (ART 85)

No Deviation

OBLIGATIONS OF SECRECY (ART 90)

No Deviation

HR PROCESSING (ART 88)

No Deviation

LOCAL DPA GUIDANCE & LEGAL SOURCES

Swedish Act on the Protection of Personal Data

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

DEVIATING REQUIREMENT:

Scope of Application Carve-Out: The Swedish Act does not apply to processing personal data for journalistic, academic, or artistic purposes (Ch 1 Sec 7 of the Swedish Act).

UNITED KINGDOM

CHART INSTRUCTIONS:

✗ Local law does not deviate from the GDPR.
✓ Local law deviates from the GDPR.

NAME

Data Protection Bill

STATUS: ADOPTED

SME EXCEPTION

N/A

LAWFULNESS OF PROCESSING (ART 6)

✓

SPECIFYING REQUIREMENT: Processing of personal data that is necessary for the performance of a task carried out in the public interest or in the exercise of the controller's official authority includes processing of personal data that is necessary for: (1) the administration of justice, (2) the exercise of a function of either House of Parliament, (3) the exercise of a function conferred on a person by an enactment or rule of law, (4) the exercise of a function of the Crown, a Minister of the Crown or a government department, or (5) an activity that supports or promotes democratic engagement (Clause 8, UK Data Protection Act 2018)

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 counselling services (Clause 9 UK Data Protection Act 2018)

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

✗

No Deviation

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; (7) substantial public interest condition; or (8) is necessary for an insurance purposes (Clauses 10(4), (5) and Schedule 1, Part 3 UK Data Protection Act 2018).

INFORMATION OBLIGATION (ART 13 & 14)

✗

No Deviation

AUTOMATED INDIVIDUAL DECISION-MAKING (ART 22)

No Deviation

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 audit functions; (6) discharging a relevant function of the Bank of England; (7) discharging regulatory functions relating to legal, health, and children's services; (8) functions of certain other regulatory bodies; (9) avoiding infringement of parliamentary privilege; (10) assessing a person's suitability for judicial appointment or in the context of judicial independence and judicial proceedings; (11) in the context of Crown honors, dignities, and appointments; (12) protection of the rights of others; (13) for a purpose that meets the health data, social work data, or education data test if performed by a qualified health worker, social worker, or education worker; (14) legal professional privilege; (15) avoiding self-incrimination; (16) corporate finance service; (17) prejudiced business activity; (18) negotiations between the data subject and controller; (19) confidential references given to the controller; (20) information recorded in the context of exams; (21) incompatibility with the publication of journalistic, academic, literal, or artistic material in the public interest; (22) statistical or scientific and historical, or archiving in the public interest, in the case of health, social work, and education data; (23) when the data are processed by a court; (24) as a result of the data subject's expectations or wishes; (25) when disclosure would lead to serious harm (for health data); (26) when an appropriate professional must give prior opinion; (27) in the case of child abuse data; (28) when it would not be in the best interests of the data subject to disclose; (29) human fertilization and embryology information; (30) adoption records and reports; (31) statements of special educational needs; (32) parental order records and reports; (33) information provided in the context of the Children's Hearings Act; and (34) as enacted by way of regulations made by the Secretary of State where necessary and proportionate to safeguard certain objectives of general public interest (Clause 15-16 and Schedules 2–4 UK Data Protection Act 2018).

JOINT CONTROLLER RESPONSIBILITIES (ART 26 (1))

No Deviation

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. (Clause 41, UK Data Protection Act 2018)

SECURITY OF PROCESSING (ART 32)

VARYING REQUIREMENT: Article 32 GDPR does not apply when processing for national security or defence purposes. In these cases, the controller or processor must implement security measures appropriate to the risks arising from the processing of the personal data. (Clause 28 UK Data Protection Act 2018).

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 honours and dignities are 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) exam scripts and marks; (13) research and statistics; and (14) archiving in the public interest (Schedule 11 UK Data Protection Act 2018).

It is required to communicate the nature of a data breach to the data subject (Clause 68(2)(a) UK Data Protection Act 2018). 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 68(7) UK Data Protection Act 2018).

DATA PROTECTION IMPACT ASSESSMENT (ART 35)

VARYING REQUIREMENT: The supervisory authority does not have the authority to establish a public list of the kinds of processing operations which are or are not subject to a data protection impact assessment. (Schedule 6 Clause 27, UK Data Protection Act 2018)

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 69(1) UK Data Protection Act 2018). Clause 71(2) UK Bill lays down a non-exhaustive list of specific tasks to be performed by the DPO when monitoring compliance with controller policies.

CERTIFICATION (ART 42)

No Deviation

DATA TRANSFER DEROGATIONS (ART 49(5))

No Deviation

POWERS SUPERVISORY AUTHORITIES (ART 58)

VARYING REQUIREMENT: The commissioner's powers under the GDPR are subject to safeguards provided for in the Act: (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;(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 115 UK Data Protection Act 2018). The commissioner has the power to inspect personal data in accordance with international obligations (Clause 119 UK Data Protection Act 2018). The commissioner has the power to issue information, assessment, enforcement, and penalty notices (Clauses 142-153 and 155-159 UK Data Protection Act 2018). The commissioner's powers of entry and inspection may only be exercised upon court approval or warrant (Schedule 15 UK Data Protection Act 2018). The commissioner has the power to inspect personal data where the inspection is necessary to discharge an international obligation of the UK, and if the personal data is either (a) processed wholly or partly by automated means, or (b) if it forms or is intended to form part of a filing system (Clause 119, UK Data Protection Act 2018).

CLASS ACTIONS (ART 80 (2))

SPECIFYING REQUIREMENT: The Secretary of State may only provide that a body, organization, or association may, independently of a data subject's mandate, have the right to lodge in the UK a complaint with the commissioner by making regulations under the UK Act (Part 7 Clause 190, Schedule 6 Part 1 Clause 53, UK Data Protection Act 2018)

ADMINISTRATIVE SANCTIONS (ART 83)

No Deviation

PENALTIES (ART 84)

No Deviation

FREEDOM OF EXPRESSION & INFORMATION (ART 85)

No Deviation

HR PROCESSING (ART 88)

VARYING REQUIREMENT: The UK Bill omits Art 88 GDPR (see Schedule 6, Clause 61 UK Data Protection Act 2018).

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. (Schedule 2 Part 6, UK Data Protection Act 2018)

OBLIGATIONS OF SECRECY (ART 90)

VARYING REQUIREMENT: The UK Bill omits Art 90 GDPR (see Schedule 6, Clause 63, UK Data Protection Act 2018)

LOCAL DPA GUIDANCE & LEGAL SOURCES

UK DATA PROTECTION ACT 2018

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.