# Cypriot Implementation of the GDPR

by Alexandros Georgiades, Ioanna Sapidou of Chrysostomides with Practical Law Data Privacy Advisor
Law stated as of 05 Feb 2020 • Cyprus

*A Practice Note discussing the requirements of Cyprus's Law Providing for the Protection of Natural Persons with Regard to the Processing of Personal Data and for the Free Movement of Such Data of 2018 (Law No. 125(1)/2018), which implements the EU General Data Protection Regulation (GDPR). This Note discusses the applicability of Cypriot data protection law and key provisions that differ from the GDPR's requirements, such as limitations on data subjects' rights and processing rules for special categories of personal data, criminal conviction and offense data, national identification numbers, and data used for archiving purposes or scientific or historical research.*



The **EU General Data Protection Regulation (Regulation (EU) 2016/679)** (GDPR), which took effect on May 25, 2018, applies directly in each **EU member state**. The GDPR replaced the **EU Data Protection Directive (Directive 95/46/EC)** (EU Directive) and the EU member state laws implementing the EU Directive. The GDPR introduced a single legal framework across the EU. However, the GDPR includes several provisions allowing EU member states to enact national legislation specifying, restricting, or expanding some requirements.

Cyprus enacted the Law Providing for the Protection of Natural Persons with Regard to the Processing of Personal Data and for the Free Movement of Such Data of 2018 (Law No.125(1)/2018) (July 31, 2018) (Personal Data Law), which aligns Cypriot data protection law with the GDPR. The Personal Data Law repeals the

 

Processing of Personal Data (Protection of Individuals) Law (Law 138 (I)/2001). Directives issued by the Office of the Commissioner for Personal Data Protection (Commissioner) under the provisions of the previous law continue to be valid until their expiration or replacement and are listed on the Commissioner's website (in Greek).

This Note discusses the applicability of the Cypriot Personal Data Law and key provisions that differ from the GDPR, including requirements on:

- Confidentiality obligations applicable to data protection officers.
- Processing special categories of personal data and criminal conviction and offense data.
- The age of child consent.
- Limiting the scope of data subjects' rights and controllers' related obligations.
- Processing for journalistic purposes or academic, artistic, or literary expression.
- Processing national identification numbers.
- Processing personal data for scientific, historical research, or statistical purposes and archiving purposes in the public interest.

## Applicability of the GDPR and Cypriot Law

The GDPR includes a territorial scope provision in Article 3 that states when it applies (see Practice Note, Determining the Applicability of the GDPR). Some personal data laws passed by EU member states include a territorial scope provision that mirrors Article 3 of the GDPR. Instead of including a territorial scope provision, the Personal Data Law states that it applies according to GDPR Article 3 (Section 3, Personal Data Law). The Personal Data Law and the GDPR apply to:

- Controllers and processors with an establishment in Cyprus that process personal data in the context of that establishment, regardless of whether the data processing takes place in the EU.
- Controllers and processors not established in the EU that process personal data about data subjects residing in Cyprus when the processing activities relate to:
  - offering goods or services to data subjects residing in Cyprus, regardless of whether they require payment; or
  - monitoring their behavior that takes place in Cyprus.
- Persons not established in Cyprus but located in a place where Cypriot law applies according to public international law.

(Section 3, Personal Data Law; Article 3, GDPR.)

## Data Protection Officers

The GDPR requires controllers and processors to appoint a data protection officer (DPO) under certain circumstances (Article 37(1), GDPR; see Practice Note, Data protection officers under the GDPR and DPA 2018). The GDPR allows EU member states to require DPO appointments in additional situations (Article 37(4), GDPR).

The Personal Data Law authorizes the Commissioner to publish a list specifying additional obligations to appoint a DPO (Section 14(2), Personal Data Law). The Commissioner has not issued any list to date. The Commissioner may publish a list of controllers and processors who have appointed DPOs, including their contact details, on the Commissioner's website, subject to the individuals' consent (Section 14(3), Personal Data Law).

The Personal Data Law binds the DPO to professional secrecy and confidentiality obligations while performing the DPO's functions, subject to any applicable professional secrecy or confidentiality laws (Section 15(1), Personal

 

Data Law).

The professional secrecy and confidentiality duties do not affect the Commissioner's investigative powers under GDPR Article 58(1) and Section 25(a) and (b) of the Personal Data Law (Section 15(2), Personal Data Law).

## Processing Special Categories of Personal Data

The GDPR prohibits processing special categories of personal data unless an exception applies (Article 9(1), GDPR). Special categories of personal data include:

- Racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data.
- Data concerning health or sex life.
- Sexual orientation.

(Article 9(1), GDPR.)

### *GDPR Exceptions Permitting Processing*

GDPR Article 9(2) includes several exceptions to the prohibition on processing special categories of personal data. Some of these exceptions require controllers to consult EU or member state law to determine a lawful basis for processing.

The exceptions requiring a basis in EU or member state law include when the processing is necessary for:

- Carrying out the controller's obligations and exercising the controller's or data subjects' rights in the fields of employment law, social security, and social protection (Article 9(2)(b), GDPR).
- Reasons of substantial public interest (Article 9(2)(g), GDPR).
- Purposes of preventive or occupational medicine to assess a data subject's working capacity, medical diagnosis, or for the provision of health or social care or treatment, the management of health or social care systems and services, or under a contract with a healthcare professional (Article 9(2)(h), GDPR).
- Reasons of public interest in the area of public health (Article 9(2)(i), GDPR).
- Archiving in the public interest, scientific or historical research purposes, or statistical purposes (Article 9(2)(j), GDPR).

Other GDPR Article 9 exceptions provide a sufficient legal basis for processing special categories of personal data under the GDPR without the need for a further basis in EU or member state law, including when the data subject consents to processing (Article 9(2)(a), (c), (d), (e), (f), GDPR).

EU or member state law may prohibit the use of data subject consent as a legal basis for processing special categories of personal data (Article 9(2)(a), GDPR). However, the Personal Data Law does not prohibit this.

For more on processing special categories of personal data, see Practice Note, Overview of EU General Data Protection Regulation: Special categories of personal data.

 

### *Cypriot Law Exceptions That Permit Processing Special Categories of Personal Data*

The Personal Data Law permits processing special categories of personal data under GDPR Article 9 when:

- Carried out to publish or issue a court decision (Section 6, Personal Data Law).
- Necessary to deliver justice (Section 6, Personal Data Law).
- Carried out for journalistic purposes or for academic, artistic, or literary expression in certain circumstances (Section 29, Personal Data Law; see Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression).
- Combining two or more large-scale public authority databases, provided certain requirements are met (Section 10(2), Personal Data Law; see Processing National Identification Number).

The Personal Data Law also includes provisions introducing further restrictions, limitations, or requirements for processing genetic and biometric data (see Genetic, Biometric, and Health Data).

The Personal Data Law permits the transfer of special categories of personal data to a non-EU country or international organization provided certain conditions are met when the international transfer is based on:

- Appropriate safeguards (Article 46, GDPR; see International Data Transfers Based on Appropriate Safeguards and Binding Corporate Rules).
- Binding corporate rules (Article 47, GDPR; see International Data Transfers in the Absence of an Adequacy Decision).
- Derogations (Article 49, GDPR; see International Data Transfers Based on GDPR Article 49 Derogations).

All other processing relating to special categories of personal data must comply with GDPR Article 9 (see GDPR Exceptions Permitting Processing). Controllers should consult other national laws to determine the legal basis for processing under GDPR Article 9(2)(b), (g), (h), (i), and (j).

### *Genetic, Biometric, and Health Data*

The GDPR permits EU member states to introduce further conditions and limitations on processing genetic, biometric, and health data (Article 9(4), GDPR).

The Personal Data Law prohibits processing genetic and biometric data for life and health insurance purposes (Section 9(1), Personal Data Law).Where the controller relies on consent to process genetic and biometric data, any further processing of these data categories requires a separate consent from the data subject (Section 9(2), Personal Data Law; see Processing for Secondary Purposes).

The Commissioner has also issued an Opinion (Opinion 2/2018) on the use of video surveillance and biometric data in the workplace (in Greek; see Workplace Surveillance).

## Processing Criminal Conviction and Offense Data

The GDPR only permits processing personal data relating to criminal convictions or offenses when either:

- Carried out under the control of official authority, for example, the police.
- Authorized by EU or member state law providing for appropriate safeguards for data subjects.

(Article 10, GDPR.)

 

The Personal Data Law permits processing criminal conviction and offense data both:

- For journalistic purposes and for academic, artistic, or literary expression in certain circumstances (see Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression).
- When combining two or more large-scale public authority databases, provided certain requirements are met (Section 10(2), Personal Data Law; see Processing National Identification Number).

The Law on the Use of Passenger Name Record Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offenses and Serious Crime, which implements Directive 2016/681/EU (PNR Directive), authorizes the processing of certain personal data categories to prevent criminal activities. A discussion of the PNR Directive is outside of the scope of this Note.

All other processing relating to criminal conviction and offense data must comply with GDPR Articles 5 and 6.

## Processing for Secondary Purposes

The GDPR generally restricts data processing to the original collection purpose unless an exception applies, for example:

- The data subject consents to processing for a secondary purpose.
- An EU or member state law, which is a necessary and proportionate measure to safeguard certain important objectives, permits the processing for a secondary purpose (see GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights).

(Article 6(4), GDPR.)

The Personal Data Law permits controllers who rely on consent to process genetic and biometric data to further process these data categories, provided data subjects provide a separate consent for the secondary processing (Section 9(2), Personal Data Law; see Genetic, Biometric, and Health Data).

In all other circumstances and without data subject consent, any secondary processing purpose must both:

- Remain compatible with the original processing purpose.
- Satisfy the conditions in GDPR Article 6(4).

To determine the secondary processing purpose's compatibility, the controller should consider the criteria specified in GDPR Article 6(4) (see Practice Note, Overview of EU General Data Protection Regulation: Further compatible processing).

## Child Consent

For online service providers offering services directly to children (called information society services in the GDPR), the GDPR permits EU member states to lower the age of child consent below 16 years old, provided the age is not lower than 13 (Article 8(1), GDPR). The Personal Data Law reduces the age of child consent to 14 (Section 8(1), Personal Data Law). For children younger than 14, personal data processing is lawful only if the person with parental responsibility gives consent (Section 8(2), Personal Data Law).

The Personal Data Law does not change the requirements for obtaining valid consent from children or impose any additional requirements or restrictions on processing personal data about children.

 

# Data Subjects' Rights

The GDPR grants data subjects several rights and imposes several obligations on controllers relating to those rights in Articles 12 to 22, 34, and 5 (as it relates to the rights and obligations in Articles 12 to 22) (see Practice Note, Data Subject Rights Under the GDPR). The GDPR permits EU member states to restrict the scope of these data subject rights and controller obligations when the restriction is a necessary and proportionate measure to safeguard certain objectives (Article 23, GDPR).

## *GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights*

EU member states may restrict the scope of data subjects' rights and controllers' related obligations in GDPR Articles 12 to 22, 34, and 5 (as it relates to the rights and obligations in Article 12 to 22) when the restriction is a necessary and proportionate measure to safeguard:

- National security.
- Defense.
- Public security.
- The prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties.
- Other important economic or financial public interests of the EU or member state, including:
  - monetary, budgetary, and taxation matters;
  - public health; and
  - social security.
- Judicial independence and proceedings.
- The prevention, investigation, detection, and prosecution of ethics breaches for regulated professions.
- Monitoring, inspection, or regulatory functions connected to the exercise of official authority regarding:
  - national or public security;
  - defense;
  - other important public interests;
  - crime prevention; or
  - breaches of ethics for regulated professions.
- Protection of the individual or the rights and freedoms of others.
- Enforcing civil law matters.

(Article 23(1), GDPR.)

EU or member state laws restricting data subjects' rights to ensure GDPR Article 23 objectives should include provisions on, when relevant:

- Purposes of the processing or categories of processing.
- Categories of personal data.
- Scope of the restrictions.
- Safeguards to prevent abuse or unlawful access or transfer.
- Specification of the controller or categories of controllers.
- Data retention periods and applicable safeguards, considering the nature, scope, and purposes of processing or categories of processing.
- Risks to the rights and freedoms of data subjects.
- Data subjects' rights to be informed about restrictions unless doing so is prejudicial to the restriction's purpose.

(Article 23(2), GDPR.)

 

## *Cypriot Law Exceptions to Data Subject Rights*

The Personal Data Law permits controllers to vary or restrict the following data subject rights or related controller obligations when necessary to safeguard GDPR Article 23 objectives, provided the controller meets certain conditions (see GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights):

- Transparency obligations (Article 12, GDPR).
- Processing restriction right (Article 18, GDPR).
- Notification obligation relating to rectification and erasure requests (Article 19, GDPR).
- Data portability right (Article 20, GDPR).
- Data breach notification obligation (Article 34, GDPR; see Data Breach Notification Right).

(Section 11(1), Personal Data Law.)

Before restricting these rights or obligations, a controller must:

- Perform a data protection impact assessment (DPIA), which must include:
  - the information provided under GDPR Articles 23(2) and 35(7); and
  - a description of the appropriate technical and organizational measures set out in GDPR Articles 24, 25, 28, and 32, where appropriate.
- Consult with the Commissioner.

(Section 11(2), (3), Personal Data Law.)

The controller must notify data subjects about any restrictions to their rights, subject to GDPR Article 14(5), which states that the requirement to provide certain information to data subjects when collecting their data from a third party does not apply in certain situations (Section 11(4), Personal Data Law).

Controllers may determine how to restrict data subjects' rights or their own obligations. However, the Commissioner may impose terms and conditions on the controller relating to:

- Any restrictive measures imposed by the controller under Personal Data Law Section 11(1).
- The information provided to the data subject under Personal Data Law Section 11(4).

(Section 11(5), Personal Data Law.)

If the restriction of rights relates to processing entrusted to a processor, the restrictions are implemented subject to the GDPR's obligations for processors under GDPR Article 28 (Section 11(1), Personal Data Law).

In addition, under the Personal Data Law, the following rights and obligations may not apply under limited circumstances when processing personal data for journalistic or academic purposes or for artistic or literary expression:

- The obligation to provide notice to a data subject when the controller obtains a data subject's personal data from a third party (Article 14, GDPR).
- The data subject's right of access (Article 15, GDPR).

(Section 29(2), Personal Data Law; see Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression).

## Data Breach Notification Right

The GDPR requires notification of data breaches to data subjects and the relevant supervisory authority under

 

certain circumstances (Articles 33 and 34, GDPR; see Practice Note, Data breach notification (GDPR and DPA 2018) (UK)). The Personal Data Law exempts controllers, in part or in whole, from the obligation to notify data subjects for the objectives stated in GDPR Article 23(1) (Section 12, Personal Data Law; see GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights).

For the exemption to apply, the controller must:

- Perform a DPIA, which must include:
  - the information provided under GDPR Articles 23(2) and 35(7); and
  - a description of the appropriate technical and organizational measures set out in GDPR Articles 24, 25, 28, and 32, where appropriate.
- Consult with the Commissioner.

(Section 11(2), (3), Personal Data Law.)

The Commissioner may impose terms and conditions on the controller's reliance on this exemption (Section 12(4), Personal Data Law).

## Derogations for Specific Processing Situations

The GDPR provides additional rules that apply to seven specific processing situations (Articles 85 to 91). These Articles permit EU member states to enact further rules that apply to the specified processing types. The Personal Data Law introduces additional rules that apply to processing:

- For journalistic purposes and academic, artistic, or literary expression (see Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression).
- National identification numbers (see Processing National Identification Number).
- For scientific or historical research, statistical purposes, or archiving in the public interest (see Processing for Scientific or Historical Research, Statistical Purposes, or Archiving in the Public Interest).
- Disclosures of personal data in official documents (see Disclosures of Personal Data in Official Documents).

### *Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression*

The Personal Data Law permits processing personal data, special categories of personal data, and criminal conviction and offense data for journalistic purposes or academic, artistic, or literary expression, provided these purposes:

- Are proportionate to the aim pursued.
- Respect the political, social, and economic rights protected by the EU Charter of Fundamental Rights, the European Convention of Human Rights, and the Constitution of Cyprus.

(Section 29(1), Personal Data Law, which implements Article 85, GDPR.)

The obligation to provide notice to a data subject when the controller obtains a data subject's personal data from a third party (Article 14, GDPR) and the data subject's right of access (Article 15, GDPR) apply when processing for these purposes, provided these rights and obligations do not impair the right to freedom of expression and information and journalistic secrecy (Section 29(2), Personal Data Law; see Cypriot Law Exceptions to Data Subject Rights).

 

## *Processing National Identification Number*

The Personal Data Law permits the combination of two or more public authority databases for public interest reasons, if the processing is necessary for either:

- Complying with a legal obligation or performing a task carried out in the public interest (Article 6(1)(c), (e), GDPR).
- Reasons of substantial public interest, purposes of preventative or occupational medicine to assess the working capacity of a data subject, medical diagnosis, or for the provision of health or social care or treatment, or reasons of public interest in the area of public health (Article 9(2)(g), (h), (i), GDPR).

(Section 10(1), Personal Data Law.)

Where the combination of two or more public authority databases relates to special categories of personal data or criminal conviction and offense data, or will be combined using identity card numbers or any other general identifier, the Personal Data Law requires controllers to both:

- Perform a DPIA.
- Consult with the Commissioner prior to processing.

(Section 10(2), Personal Data Law, which implements Article 87, GDPR.)

The public authorities or bodies intending to combine their databases must perform the DPIA jointly, which must include both:

- The information provided under GDPR Articles 23(2) and 35(7).
- A description of the appropriate technical and organizational measures set out in GDPR Articles 24, 25, 28, and 32, where appropriate.

(Section 10(3), Personal Data Law.)

The Commissioner may impose terms and conditions for the combination of the databases (Section 10(4), Personal Data Law).

## *Processing for Scientific or Historical Research, Statistical Purposes, or Archiving in the Public Interest*

Under the Personal Data Law, a controller or data processor that processes personal data for scientific or historical research, statistical purposes, or archiving in the public interest must not make a decision based on that processing that produces legal or other similarly significant effects for the data subject. (Section 31, Personal Data Law, which implements Article 89, GDPR.)

## *Disclosures of Personal Data in Official Documents*

Under the Personal Data Law, public authorities and bodies processing personal data in official documents to perform a task in the public interest must only disclose the personal data consistent with the Right of Access to Public Sector Documents Law (Section 30, Personal Data Law, which implements Article 86, GDPR).

 

### *Secrecy Obligations*

The GDPR permits EU member states to adopt rules specifying the powers of supervisory authorities regarding controllers and processors that are subject to:

- An obligation of professional secrecy.
- Another equivalent secrecy obligation.

(Article 90, GDPR.)

The Personal Data Law allows the Commissioner access to all personal data and information, including confidential information, required for the Commissioner to perform its tasks and exercise its powers. The Commissioner's right of access does not extend to information protected by legal professional privilege. (Section 25, Personal Data Law, which implements Article 90, GDPR.)

The DPOs obligation to professional secrecy or confidentiality will not prevent the disclosure of information by the DPO to the Commissioner when exercising the investigative powers of the Commissioner provided for in GDPR Article 58(1) and Personal Data Law Section 25(a) and (b) (Section 15(2), Personal Data Law).

For more information on the powers of the Commissioner, see Supervisory Authority.

## Processing in the Employment Context

The GDPR permits EU member states, by law or by collective agreements, to provide more specific rules on processing personal data in the employment context (Article 88, GDPR). The Personal Data Law does not provide for more specific rules relating to the processing of personal data in the employment context.

However, the Commissioner has issued a Directive for the Processing of Personal Data in the Context of Employment Relations (2005) (in Greek) regarding the processing of personal data in the context of employment relations which is binding. The Commissioner has also issued:

- Guidelines (No. 4/2017) for public sector controllers regarding the right of access by employees or candidates (in Greek).
- Opinion 1/2018 for trade unions regarding notification by employers of employees' salary and trade union contribution amounts (in Greek).
- Opinion 2/2018 regarding the use of video surveillance and biometric data in the workplace (in Greek; see Workplace Surveillance).
- Opinion 1/2019 regarding access to employees' and former employees' email account (in Greek).
- An announcement (in Greek) regarding the use of polygraph testing during recruitment and in the workplace.

### *Employee Consent*

Employers should use caution when relying on consent in the employment context. EU supervisory authorities, including the Commissioner, do not generally consider consent given in the employment context as freely given and often consider it invalid. Consent must comply with GDPR Articles 7 (Conditions for consent) and 6(1)(a), which require data subjects to give consent for specified purposes. For more on employee consent under the GDPR, see Practice Note, Employee Consent Under the GDPR.

 

### *Workplace Surveillance*

The Commissioner has published Opinion 2/2018 on the use of video surveillance and biometric data in the workplace (in Greek). The Opinion permits workplace surveillance in limited circumstances, provided the employer can establish:

- The lawfulness and necessity of the surveillance.
- The use of less invasive measures would not achieve the purpose.

Video surveillance may be permitted in limited circumstances when:

- Justified by the specific working conditions.
- Necessary to protect employee's health and security.
- Necessary to ensure safety in critical working environments, such as military factories and banks.

Controllers should limit video surveillance to points of entry and exit, outside elevators, parking garages, cashiers, or areas where safes are located and should focus cameras on the protected object and not on employees' faces. Employers should not install cameras in employees' offices, conference rooms, corridors, kitchen, restrooms, or dressing rooms.

Employers must not use video surveillance data as the sole criteria for assessing employees' behavior and performance.

## Other GDPR Derogations

### *Supervisory Authority*

Chapter 8 of the Personal Data Law establishes the role of the Commissioner for Personal Data Protection (Commissioner) (Sections 19 to 22, Personal Data Law, which implement Articles 51 and 54, GDPR).

In addition to the duties provided for in GDPR Article 57, the Commissioner shall:

- Exercise the duties and powers conferred on the Commissioner's office by the GDPR, Personal Data Law, and any other law.
- Authorize any officer of the Commissioner's office in a position of authority to exercise powers on the Commissioner's behalf, to the extent set out in the Commissioner's authorization.
- Publicize a case concerning the performance of the Commissioner's duties or powers. Where the case concerns cross-border processing, the Commissioner will consult with the lead authority.
- Publish on the Commissioner's website the ways of submitting complaints and applications.
- Examine complaints and, where possible, depending on a complaint's nature and type, the Commissioner must inform the complainant in writing of the progress and outcome of the complaint within 30 days of the submission. If the complaint is unfounded or does not fall within the responsibilities of the Commissioner, the Commissioner must inform the complainant in writing within 30 days of the submission of the complaint.
- Inform, where appropriate, the data subject, controller, and processor about the time limits provided in the GDPR (Articles 60 to 66, GDPR).
- Not examine a complaint or discontinue its examination for public interest reasons and notify the data subject within a reasonable time about the reasons for non-examination or for discontinuation of the examination of the complaint.
- Draw up and make public the list of processing operations and cases requiring the appointment of a DPO and may make a list of controllers and processors who have designated a DPO available on the Commissioner's website.

 

(Articles 23 and 24, Personal Data Law.)

The Commissioner is not competent to supervise processing by courts acting in their judicial capacity (Section 23(4), Personal Data Law).

In addition to the powers specified in GDPR Article 58, the Commissioner has several additional enforcement and investigation powers under Section 25 of the Personal Data Law. These powers include, for example:

- The right to access to all personal data and information, including confidential information, required for the Commissioner to perform its tasks and exercise its powers, subject to the requirements of GDPR Article 58(1)(a) and (e), GDPR. This access right does not extend to information protected by legal professional privilege.
- The power to enter business premises unannounced, subject to GDPR Article 58(1)(f). This power does not extend to residences.
- The right to assistance by an expert or the police for the exercise of investigative powers under GDPR Article 58(1).
- The power to seize documents or electronic equipment with a search warrant.

In addition to the authorization and advisory powers provided for in Article 58(3), GDPR, the Commissioner has the power to:

- Authorize and impose terms and conditions on the combination of filing systems (Section 10, Personal Data Law; see Processing National Identification Number).
- Impose terms and conditions on controllers relating to their restriction of data subjects' rights (Section 11, Personal Data Law; see Cypriot Law Exceptions to Data Subject Rights).
- Impose terms and conditions on controllers relating to data breach notification exemptions (Section 12, Personal Data Law; see Data Breach Notification Right).
- Impose limits on the transfer of special categories of personal data (Sections 17 and 18, Personal Data Law; see International Data Transfers in the Absence of an Adequacy Decision).
- Recommend to the Minister of Justice and Public Order (Minister) the conclusion of agreements with other countries under international co-operation mechanisms set out in GDPR Article 50.
- Conclude, establish, and sign memoranda of understanding with other supervisory authorities or international organizations on international co-operation (Section 35, Personal Data Law).
- Notify the Attorney General, the police, or both, of any breach of the GDPR or Personal Data Law that may constitute an offense under Section 33 of the Personal Data Law.

The Commissioner can confer powers, including investigative powers, to employees of other member state supervisory authorities who participate in joint operations with the Commissioner in Cyprus (Section 27, Personal Data Law).

## *Administrative Fines and Criminal Penalties*

The GDPR permits EU member states to specify penalties for GDPR violations that are not subject to administrative fines under GDPR Article 83 (Article 84, GDPR). The Personal Data Law establishes several criminal offenses punishable by a fine of up to:

- EUR30,000 or up to three years' imprisonment or both for a breach of Section 33(1)(a) to (l) (Section 33(2), Personal Data Law).
- EUR10,000 or up to one years' imprisonment or both for a breach of Section 33(1)(m) and (n) (Section 33(3), Personal Data Law).
- EUR50,000 or up to five years' imprisonment or both for a breach of Section 33(1)(g) to (j), where the offense hinders the interests of the State or the operation of Government or threatens security (Section 33(4), Personal Data Law).

 

The Personal Data Law provides for criminal offenses in the following cases:

- A controller or processor:
  - failing to maintain or update records of processing activities under GDPR Article 30;
  - refusing to disclose those records to the Commissioner; or
  - providing false, inaccurate, misleading, or insufficient information regarding those records to the Commissioner (Section 33(1)(a), Personal Data Law).
- A controller or processor failing to cooperate with the Commissioner under GDPR Article 31 (Section 33(1)(b), Personal Data Law).
- A controller failing to notify a breach to the Commissioner under GDPR Article 33(1) (Section 33(1)(c), Personal Data Law).
- A processor failing to notify a controller of a data breach without undue delay under GDPR Article 33(2) (Section 33(1)(d), Personal Data Law).
- A controller failing to notify a data subject of a data breach under GDPR Article 34 (Section 33(1)(e), Personal Data Law).
- A controller failing to perform a DPIA, in breach of GDPR Article 35(1) or Personal Data Law Section 13 (Section 33(1)(f), Personal Data Law).
- Where a controller or processor prevents a DPO from performing their duties, particularly duties relating to cooperation with the Commissioner (Section 33(1)(g), Personal Data Law).
- Where a certification body accredits or fails to revoke an accreditation under GDPR Article 42 (Section 33(1)(h), Personal Data Law).
- Where a controller or processor transfers personal data to a non-EU country or international organization in breach of GDPR Chapter V (Section 33(1)(i), Personal Data Law).
- Where a controller or processor transfers personal data to a non-EU country or international organization in breach of restrictions imposed by the Commissioner under the Personal Data Law (Section 33(j), Personal Data Law).
- In relation to any person who unlawfully interferes with a filing system of personal data or receives knowledge of that personal data or removes, alters, harms, destroys, processes, exploits, broadcasts, announces, grants access to, or allows unauthorized persons to obtain personal data for any purpose (Section 33(1)(k), Personal Data Law).
- The prevention or obstruction by a controller or processor of the performance of the Commissioner's powers under GDPR Article 58 and Personal Data Law Section 17 (Section 33(1)(l), Personal Data Law).
- Non-compliance with the Personal Data Law or the GDPR in relation to personal data processing that is not covered by one of the other offenses listed (Section 33(1)(m), Personal Data Law).
- Where a public authority or public body combines a large-scale filing system in breach of the Personal Data Law's requirements (Section 33(1)(n), Personal Data Law).
- Where the controller or processor is:
  - an undertaking or group of undertakings, criminal liability rests with the chief executive body of the undertaking or group of undertakings concerned; or
  - a public authority or body, criminal liability rests with the head of the public authority or body or the person that carries out effective management of the public authority or body.

(Section 33(5), Personal Data Law.)

For more on enforcement and sanctions under the GDPR, see Practice Note, GDPR and DPA 2018: enforcement, sanctions and remedies (UK).

## *Public Authorities and Bodies*

Public authorities or public bodies may be fined up to EUR200,000 for breaches relating to non-profitable activities (Section 32(3), Personal Data Law).

 

## *International Data Transfers in the Absence of an Adequacy Decision*

The GDPR permits EU member states to restrict the transfer of specific categories of personal data to countries outside of the EU for public interest reasons when there is no adequacy decision for the recipient country (Article 49(5), GDPR).

### International Data Transfers Based on Appropriate Safeguards and Binding Corporate Rules

Before transferring special categories of personal data to a non-EU country or international organization based on appropriate safeguards under GDPR Article 46 or binding corporate rules under GDPR Article 47, the Personal Data Law requires a controller or processor to inform the Commissioner of the data transfer (Section 17(1), Personal Data Law).

The Commissioner may, for important public interest reasons, impose restrictions on the transfer of special categories of personal data to a non-EU country or to international organizations (Section 17(2), Personal Data Law).

### International Data Transfers Based on GDPR Article 49 Derogations

Before transferring special categories of personal data to a non-EU country or international organization based on the GDPR Article 49 derogations, the Personal Data Law requires a controller or processor to:

- Perform a DPIA, which must include:
  - the information provided under GDPR Article 35(7); and
  - a description of the appropriate technical and organizational measures set out under GDPR Articles 24, 25, 28 and 32, if appropriate.
- Consult with the Commissioner.

(Section 18(1), (2), Personal Data Law.)

The Commissioner may, for important public interest reasons, impose restrictions on the transfer of special categories of personal data to a non-EU country or international organizations (Section 18(3), Personal Data Law).

**PERSONAL DATA LAW AND GDPR STATUTORY REFERENCES**

| Subject Matter | Personal Data Law Section | GDPR Article Permitting Member State Derogation |
|---|---|---|
| Applicability of Cypriot law (see Applicability of the GDPR and Cypriot Law) | 3 | |
| Appointing a data protection officer (see Data Protection Officers) | 14(2), (3) | 38(5) |

 

| | | |
|---|---|---|
| Requirements for processing special categories of personal data (see Processing Special Categories of Personal Data) | 6,7 and 31 | 9(2)(b), (g), (h), (i), (j) |
| Requirements for processing genetic, biometric, and health data (see Genetic, Biometric, and Health Data) | 9 | 9(4) |
| Requirements for processing criminal conviction and offense data (see Processing Criminal Conviction and Offense Data) | 29 | 10 |
| Processing for secondary purposes (see Processing for Secondary Purposes) | NA | 6(4) |
| Child consent (see Child Consent) | 8 | 8(1) |
| Limitations on data subjects' rights (see Data Subjects' Rights) | 11 | 23 |
| Requirements for processing for journalistic purposes or academic, artistic, or literary expression (see Processing for Journalistic Purposes or Academic, Artistic, or Literary Expression) | 29 | 85 |
| Requirements for processing national identification numbers (see Processing National Identification Number) | 10 | 87 |
| Requirements when processing for archiving in the public interest or for scientific, historical research, or statistical purposes (see Processing for | 31 | 89 |

| | | |
|---|---|---|
| Scientific or Historical Research, Statistical Purposes, or Archiving in the Public Interest) | | |
| Secrecy obligations (see Secrecy Obligations) | 15 | 90(1) |
| Processing employee personal data (see Processing in the Employment Context) | NA | 88 |
| Supervisory authority (see Supervisory Authority) | Chapter 8 | 51, 54 |
| Administrative fines and criminal penalties (see Administrative Fines and Criminal Penalties) | 33 | 84 |
| Public authorities and bodies (see Public Authorities and Bodies) | 32(3) | 83(7) |
| Use of video surveillance (see Workplace Surveillance) | NA | 6(2) |
| International data transfer in the absence of an adequacy decision (see International Data Transfers in the Absence of an Adequacy Decision) | 17,18 | 49(5) |

 