THOMSON REUTERS
PRACTICAL LAW™

Liechtensteinian Implementation of the GDPR

by Alja Poler de Zwart and Marijn Storm, Morrison & Foerster LLP, with Practical Law Data Privacy & Cybersecurity

Status: **Law stated as of 23-Sep-2022** | Jurisdiction: **European Union, Liechtenstein**

This document is published by Practical Law and can be found at: **uk.practicallaw.tr.com/w-034-0142**
Request a free trial and demonstration at: **uk.practicallaw.tr.com/about/freetrial**

A Practice Note discussing Liechtenstein's Data Protection Act (No. 272 of October 4, 2018) (Data Protection Act) and the Data Protection Regulation (No. 415 of December 11, 2018) (Data Protection Regulation), which implement the EU General Data Protection Regulation (GDPR). This Note addresses key requirements of the Data Protection Act and Data Protection Regulation, such as requirements to appoint a data protection officer, exceptions permitting processing special categories of personal data, data subject rights derogations including under GDPR Article 23, and derogations for specific processing situations under GDPR Articles 85 to 91.

The EU General Data Protection Regulation (Regulation (EU) 2016/679) (GDPR) took effect on May 25, 2018 and applies directly in each EU member state. The European Econimic Area (EEA) Joint Committee incorporated the GDPR into the EEA Agreement on July 6, 2018, extending the GDPR's application to Liechtenstein. The GDPR replaced the EU Data Protection Directive (Directive 95/46/EC) and 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.

Liechtenstein enacted the Data Protection Act (No. 272 of October 4, 2018) (Data Protection Act) and the Data Protection Regulation (No. 415 of December 11, 2018) (Data Protection Regulation), which:

- Align Liechtensteinian data protection law with the GDPR.
- Repeal and replace the prior data protection law (Law No. 55 (2002)) and regulations (No. 102 (2002) and No. 403 (2013)).
- Change some of the GDPR's requirements.

The Data Protection Act also implements the EU Law Enforcement Directive (Directive (EU) 2016/680) (Law Enforcement Directive), which governs personal data processing by law enforcement authorities. The details of the Law Enforcement Directive are outside the scope of this Note.

This Note discusses the applicability of Liechtensteinian data protection law and key provisions of the Data Protection Act and Data Protection Regulation, including requirements on:

- Processing special categories of personal data.
- Processing criminal conviction and offense data.
- The age of child consent.
- Limiting the scope of data subjects' rights and controllers' related obligations.
- Processing personal data for journalistic purposes.
- Processing personal data for archiving in the public interest, scientific or historical research, or statistical purposes.
- Processing in the employment context.
- Video surveillance

For more on the GDPR's application in Liechtenstein and guidance issued by the Liechtenstein Data Protection Office, see Practice Note, GDPR Data Protection Authority Guidance Tracker by Country (EEA): Liechtenstein.

Applicability of the GDPR and Liechtensteinian Law

Territorial Scope

The GDPR applies to:

- Controllers and processors that process personal data in the context of the activities of an EU establishment,

regardless of whether the data processing takes place in the EU (Article 3(1), GDPR).

- Controllers and processors not established in the EU that process personal data about data subjects in the EU when the processing activities relate to:
  - offering goods or services to data subjects in the EU, regardless of whether the controller or processor requires payment; or
  - monitoring their behavior that takes place in the EU.

  (Article 3(2), GDPR.)
- Controllers not established in the EU that process personal data and that are subject to member state law under public international law (Article 3(3), GDPR).

Some EU member states have passed national laws that include a territorial scope provision that mirrors GDPR Article 3, while other member states' laws include different applicability language or do not include a territorial scope provision. The Data Protection Act applies to non-public controllers and processors:

- Processing personal data in Liechtenstein.
- Processing personal data in the context of a Liechtensteinian establishment.
- Not established in Liechtenstein but subject to the GDPR.

(Article 2(3), Data Protection Act.)

Material Scope

The GDPR includes a material scope provision stating that it does not apply to:

- Activities that fall outside the scope of EU law.
- Processing by EU member states under Title V, Chapter 2 of the Treaty on European Union that relates to foreign and security policy.
- Processing for purely personal or household activities.
- Processing by competent authorities for preventing, investigating, detecting, or prosecuting criminal offenses and executing criminal penalties, including safeguarding against and preventing threats to public safety.

(Article 2(2), GDPR.)

The Data Protection Act also includes a material scope provision stating that it does not apply when EEA law, particularly the GDPR, directly applies (Article 2(6), Data Protection Act).

When special legal provisions regulate data protection, those provisions take precedence over the Data Protection Act. However, where those provisions do not regulate a specific matter, the Data Protection Act also applies in a subsidiary manner (Article 2(2), Data Protection Act). If the Data Protection Act does not apply because special legal provisions regulating data protection apply, only Articles 9 to 20 and 39 to 44 of the Data Protection Act apply (Article 2(3), Data Protection Act). Articles 9 to 20 and 39 to 44 of the Data Protection Act relate primarily to the Data Protection Office, enforcement, and penalties.

The Data Protection Act also applies to public bodies processing personal data. Requirements specific to public bodies are outside the scope of this Note.

For more on the GDPR's applicability and scope, see Practice Note, Determining the Applicability of the GDPR.

Data Protection Officers

The GDPR requires controllers and processors to appoint a data protection officer (DPO) under certain circumstances (Article 37(1), GDPR). The GDPR allows EU member states to require DPO appointments in additional situations (Article 37(4), GDPR). The Data Protection Act does not require appointing a DPO under additional circumstances.

The Data Protection Act binds DPOs to a professional secrecy obligation regarding data subjects' identity and any circumstances that enable the DPO to draw conclusions about a data subject, unless the data subject consents to disclosure of their information (Article 38(2), Data Protection Act). DPOs and their assistants are not required to disclose their files and documents as evidence when the data subject concerned has the right to refuse to give evidence (Article 38(3), Data Protection Act).

Controllers and processors required to appoint a DPO may only dismiss their DPO if they meet the conditions on termination without notice for cause set out in Section 1173a, Article 53 of the General Civil Code (in German) (Article 38(1), Data Protection Act).

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.)

On August 1, 2022, the EU Court of Justice (ECJ) ruled that processing personal data liable to indirectly reveal sensitive information concerning an individual is prohibited unless an exception applies, highlighting how broadly special categories of personal data are defined (*Case C-184/20: OT v Vyriausioji tarnybinės etikos komisija (Chief Official Ethics Commission, Lithuania)*; see Legal Update, Information indirectly disclosing sexual orientation is special category personal data (ECJ)).

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 field 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, assessing an employee's working capacity, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services, based on EU or member state law or under a contract with a healthcare professional, subject to certain conditions and safeguards (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, 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 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) to (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). The Data Protection Act does not prohibit this.

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

Data Protection Act Exceptions That Permit Processing Special Categories of Personal Data

The Data Protection Act permits organizations to process special categories of personal data if the processing is necessary:

- To exercise social security and social protection rights and to comply with related obligations.
- For purposes of preventive medicine, assessing an employee's working capacity, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services, or under a contract with a healthcare professional or another party with a professional secrecy obligation.
- For reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of healthcare, medicinal products, or medical devices. Controllers and processors must also comply with applicable occupational and criminal law provisions to ensure professional secrecy.

(Article 21(1)(a), Data Protection Act.)

The exceptions above replace the exemptions under GDPR Article 9(2)(b), (h), and (i). The remaining exceptions of GDPR Article 9(2) apply in full.

If the controller relies on consent to process special categories of personal data under GDPR Article 9(2)(a), the consent must explicitly mention the processing of this type of personal data (Article 51(5), Data Protection Act).

Controllers and processors processing special categories of personal data for the purposes in 21(1)(a) of the Data Protection Act must implement appropriate and specific measures to safeguard data subjects' interests, including, for example:

- Implementing technical and organizational measures to ensure that the processing complies with the GDPR.
- Measures to verify and establish whether and by whom personal data was input, altered, or removed.
- Increasing awareness of staff involved in processing operations.
- Designating a data protection officer.
- Limiting access to personal data under their control.

- Pseudonymizing personal data.
- Encrypting personal data.
- Ensuring the ability, confidentiality, integrity, availability and resilience of data processing systems and services, including the ability to rapidly restore availability and access after a physical or technical incident.
- Regularly testing, assessing, and evaluating the effectiveness of technical and organizational security measures.
- Implementing specific rules and procedures to ensure compliance with the Data Protection Act and the GDPR when engaging in data transfers and secondary processing.

(Article 21(2), Data Protection Act.)

When determining which measures to implement, controllers and processors must consider:

- The state of technological development.
- Implementation costs.
- The processing's nature, scope, context and purpose.
- The risks to data subjects' rights and freedoms.

(Article 21(2), Data Protection Act.)

The Data Protection Act also permits processing special categories of data under certain conditions for:

- Archiving in the public interest, scientific or historical research, or statistical purposes (see Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes).
- Personal, family, and genealogical research and maintaining and publishing family chronicles and biographies (see Processing for Personal, Family, or Genealogical Research or to Maintain or Publish Family Chronicles and Biographies).
- Secondary purposes (see Processing for Secondary Purposes).

Processing Criminal Conviction and Offense Data

The GDPR only permits processing personal data relating to criminal convictions and 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 Data Protection Act includes provisions implementing the Law Enforcement Directive, which governs data processing by law enforcement authorities. It also includes provisions permitting public and non-public bodies to process personal data for secondary purposes when necessary for the prosecution of crimes (Articles 22 and 23, Data Protection Act; see Processing for Secondary Purposes). The Law Enforcement Directive and provisions applicable to public bodies are outside the scope of this Note.

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 Data Protection Act permits non-public bodies to process personal data for secondary purposes if both:

- The processing is necessary to:
  - prevent threats to state or public security or to prosecute criminal offenses; or
  - establish, exercise, or defend legal claims.
- The data subject does not have an overriding interest in preventing the processing.

(Article 23(1), Data Protection Act.)

The Data Protection Act permits processing special categories of data for secondary purposes if both:

- The processing meets the conditions set out in Data Protection Act Article 23(1).
- An exception in GDPR Article 9(2) or Data Protection Act Article 21 applies.

(Article 23(2), Data Protection Act; see Processing Special Categories of Personal Data.)

The Data Protection Act also permits secondary processing of personal data and special categories of personal data for archiving in the public interest, scientific or historical research, or statistical purposes under certain circumstances (Articles 27(3) and 29(3), Data Protection Act; Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes).

All other secondary processing must comply with GDPR Article 6(4). Without data subject consent or an EU or member state law permitting the secondary processing, any secondary processing purpose must be compatible with the original processing purpose. 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).

The Data Protection Act limits a controller's obligation to provide information to data subjects under GDPR Article 13(3) in certain circumstances when it intends to process the personal data for secondary purposes (see Information Right).

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, if the age is not lower than 13 (Article 8(1), GDPR). The Data Protection Act does not reduce the age of child consent, 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 controllers' related obligations when the restriction is a necessary and proportionate measure to safeguard certain objectives or in specific processing situations (Articles 23 and 85 to 91, GDPR; see GDPR Article 23 Objectives That Permit Restrictions to Data Subject Rights and Derogations for Specific Processing Situations).

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 Articles 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 must, when relevant, include provisions on:

- Purposes of 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 data subjects' rights and freedoms.
- Data subjects' rights to be informed about restrictions, unless doing so is prejudicial to the restrictions' purposes.

(Article 23(2), GDPR.)

Data Protection Act Variations to Data Subject Rights

The Data Protection Act includes provisions limiting the scope of the following data subject rights:

- Information right (see Information Right).
- Access right (see Access Right).
- Erasure right (see Erasure Right).
- Right to object (see Right to Object).
- The right not to be subject to automated decision-making (see Automated Decision-Making).
- Data breach notification right (see Data Breach Notification Right).

The Data Protection Act also limits the scope of several data subject rights when controllers process personal data for:

- Archiving in the public interest, scientific or historical research, or statistical purposes (see Data Subject Rights Restrictions When Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes).
- Certain journalistic purposes (see Processing for Journalistic Purposes and Access Right).

Information Right

The Data Protection Act limits a controller's obligation to provide certain information to data subjects under GDPR Article 13(3) when it intends to process the personal data for secondary purposes and disclosing information on the secondary processing:

- Concerns data stored in analog form, used by the controller to directly contact the data subject through the secondary processing and:
  - the purpose is consistent with the original collection purpose;
  - the communication with the data subject does not take place in digital form; and
  - the data subject's interest in obtaining the secondary processing information is minimal, considering the individual circumstances and the context of the original data collection.

  (Article 32(1)(a), Data Protection Act.)
- Concerns a public body and the information would prevent it from properly performing its tasks relating to national security, defense, public security, or the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties, and the data subject's interests do not outweigh the controller's interests (Article 32(1)(b), Data Protection Act).
- Would put public security at risk or be detrimental to state welfare and the data subject's interests do not outweigh the controller's interests (Article 32(1)(c), Data Protection Act).
- Would impair the establishment, execution, or defense of legal claims and the data subject's interests do not outweigh the controller's interests (Article 32(1)(d), Data Protection Act).
- Would impair a confidential data transfer to public bodies (Article 32(1)(e), Data Protection Act).

If the controller does not provide information on the secondary processing to the data subject:

- Based on Data Protection Act Article 32(1)(a) to (c), the controller must:
  - take appropriate measures to protect the data subject's legitimate interests, including providing information under GDPR Article 13(1) and (2) to the public in precise, transparent, understandable, and easily accessible form with clear, simple language; and
  - record in writing the reasons it did not disclose the information.
- Due to a temporary obstacle, the controller must provide the information within a reasonable time period considering the specific circumstances of the processing, but no later than two weeks after the obstacle has resolved.

(Article 32(2), (3), Data Protection Act.)

The Data Protection Act also limits a controller's obligation to provide certain information to data subjects under GDPR Article 14(1), (2), and (4) when it has not obtained the personal data from the data subject and when providing the information:

- Concerns a public body and would:
  - prevent it from properly performing its tasks relating to national security, defense, public security, or the prevention, investigation, detection, or prosecution of criminal offenses or the execution of criminal penalties; or
  - threaten public security or order or otherwise be detrimental to the state.
- Concerns a non-public body and:
  - would impair the establishment, execution, or defense of legal claims or the processing includes data from private contracts and is intended to prevent harm from criminal offenses, unless the data subject has an overriding interest in receiving the information; or
  - the responsible public body has determined that disclosing the data would impair public security

or disadvantage the state, with the exception of processing for law enforcement purposes.

(Article 33(1), Data Protection Act.)

If the controller does not provide information to the data subject based on Data Protection Act Article 33(1), it must:

- Take appropriate measures to protect the data subject's legitimate interests, including providing information under GDPR Article 14(1) and (2) to the public in precise, transparent, understandable, and easily accessible form with clear, simple language.
- Record in writing the reasons it did not disclose the information.

(Article 33(2), Data Protection Act.)

Under the Data Protection Act, a controller's obligation to provide certain information to data subjects under GDPR Article 14 also does not apply if the information is:

- Subject to legal confidentiality obligations.
- By its nature confidential, in particular due to a third party's overriding legitimate interests.

(Article 30(1), Data Protection Act.)

Access Right

Under the Data Protection Act, data subjects' access rights under GDPR Article 15 do not apply if either:

- The controller is not required to provide information to the data subject under Data Protection Act Article 33, which provides exceptions to the controller's information obligations when it does not obtain the personal data from the data subject.
- The controller retained the personal data only because a legal or statutory provision requires retention or the personal data only serves the purpose of monitoring data protection or safeguarding data, and providing access to the personal data would involve a disproportionate effort and appropriate technical and organizational measures prevent the controller from processing it for other purposes.

(Article 34(1), Data Protection Act.)

Controllers denying a data subject's access request must:

- Document the reasons for denying the request.
- Inform the data subject of these reasons unless doing so would undermine the intended purpose of refusing to provide the information.

(Article 34(2), Data Protection Act.)

A controller's obligation to provide data subjects with access to their information under GDPR Article 15 also does not apply if doing so would disclose information that is:

- Subject to legal confidentiality obligations.
- By its nature confidential, in particular due to a third party's overriding legitimate interests.

(Article 30(1), Data Protection Act.)

In addition, the Data Protection Act permits controllers to restrict data subjects' access rights under GDPR Article 15 in certain circumstances when processing for archiving in the public interest, scientific or historical research, or statistical purposes (Articles 27(4) and 29(4), Data Protection Act; see Data Subject Rights Restrictions When Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes).

The Data Protection Act also permits controllers to deny, limit, or delay providing data subjects access to their personal data under GDPR Article 15 when the controller plans to publish it in the editorial section of periodically published media and providing access would:

- Disclose the source of the information.
- Provide insight into drafts of publications.
- Threaten the free formation of public opinion.

(Article 25(1), Data Protection Act; see Processing for Journalistic Purposes.)

Members of the press may also refuse, limit, or delay providing data subjects access to their personal data under GDPR Article 15 if they are processing the personal data exclusively as a work aid (Article 25(2), Data Protection Act).

Erasure Right

Under the Data Protection Act, data subjects' erasure rights under GDPR Article 17 do not apply if the following conditions are met:

- The processing was lawful.
- Automated or non-automated erasure would be impossible or involve a disproportionate effort due to the specific processing or storage method.
- The data subject has a minimal interest in erasing their personal data.

In these cases, the data subject's right to restrict processing under GDPR Article 18 applies instead of the erasure right. (Article 35(1), Data Protection Act.)

In addition, the data subject's right to restrict processing under GDPR Article 18 applies instead of the erasure right if both:

- The personal data is no longer necessary for the collection or processing purposes or has been unlawfully processed; and

- The controller has reason to believe erasure would adversely affect the data subject's legitimate interests.

The controller must inform the data subject of the processing restriction, unless doing so is impossible or involves a disproportionate effort (Article 35(2) Data Protection Act).

The data subjects' erasure right does not apply if contractual or legal retention periods prevent the controller from erasing the data (Article 35(3) Data Protection Act).

Right to Object

Under the Data Protection Act, a data subject's right to object to processing under GDPR Article 21(1) does not apply to a public body if either:

- An urgent public interest in the processing outweighs the data subject's interests.
- A legal provision requires the processing.

(Article 36, Data Protection Act.)

In addition, the Data Protection Act limits the right to object when controllers process personal data for archiving in the public interest, scientific or historical research, or statistical purposes (see Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes).

Automated Decision-Making

The GDPR grants data subjects the right to not be subject to a decision based solely on automated processing, including profiling, which has legal or other significant effects on the data subject (Article 22(1), GDPR). This right does not apply when the automated decision is:

- Necessary for entering into or performing a contract with the data subject.
- Authorized by EU or member state law applicable to the controller if the law requires suitable measures to safeguard the data subject's rights and freedoms and legitimate interests.
- Based on explicit data subject consent.

(Article 22(2), GDPR.)

For more on this right under the GDPR, see Practice Note, Data Subject Rights Under the GDPR: Automated Decision-Making Objection Right and Automated Decision-Making Obligations.

The automated decision-making objection right does not apply under the Data Protection Act if the controller makes the decision:

- In the context of providing services under an insurance contract and:
  - the decision determines the insurance premium;
  - fulfills a data subject's request; or
  - the decision is based on the application of binding remuneration rules for therapeutic treatment.
- To fulfill due diligence obligations for establishing a business relationship and monitoring and evaluating risk under Due Diligence Act Sections 5, 9, and 9(a).
- With regard to credit transactions under Banking Act Article 3(3)(b).
- With regard to providing an investment service or ancillary services under Banking Act Article 3(4) or Asset Management Act Article 3.

(Article 37, Data Protection Act.)

Data Breach Notification Right

Under the Data Protection Act, a controller's obligation to notify data subjects of certain data breaches under GDPR Article 34 does not apply if doing so would disclose information that is:

- Subject to legal confidentiality obligations.
- By its nature confidential, in particular due to a third party's overriding legitimate interests.

(Article 30(1), Data Protection Act.)

However, if a data subject has an overriding interest in learning about the data breach considering the threat of damage, the controller must inform the data subject of the data breach according to GDPR Article 34 (Article 30(1)(c), Data Protection Act).

Data Subject Rights Restrictions When Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes

The GDPR permits EU member states to establish rules when processing personal data for archiving in the public interest, scientific or historical research, and statistical purposes (Article 89, GDPR). The Data Protection Act permits controllers to restrict data subjects' access (GDPR Article 15), rectification (GDPR Article 16), processing restriction (GDPR Article 18), and objection (GDPR Article 21) rights when processing personal data for scientific or historical research or statistical purposes:

- To the extent they are likely to render impossible or seriously impair achieving the research or statistical purposes.
- When the restrictions are necessary to fulfill the research or statistical purposes.

(Article 27(4), Data Protection Act.)

Data subjects' access rights under GDPR Article 15 also do not apply if the data is required for scientific research and providing access would involve a disproportionate effort (Article 27(4), Data Protection Act).

When processing for archiving purposes in the public interest, the following data subject rights do not apply:

- Access rights (GDPR Article 15), if the archival material is not connected to the data subject's name or cannot be located without unreasonable administrative effort.
- Rectification rights (GDPR Article 16), if the data subject disputes the accuracy of their personal data. The data subject can present their version of the data to the archive, which must add it to the relevant files.
- Processing restriction rights (GDPR Article 18(1)(a), (b), and (d)), data portability rights (GDPR Article 20), and objection rights (GDPR Article 21) if exercising these rights is likely to render impossible or seriously impair the archiving purposes in the public interest and the exceptions are necessary to achieve those purposes.

(Article 29(4) to (6), Data Protection Act.)

Derogations for Specific Processing Situations

GDPR Articles 85 to 91 provide additional rules that apply to seven specific processing situations. These Articles permit EU member states to enact further rules that apply to the specified processing types. The Data Protection Act introduces further rules that apply to:

- Processing for journalistic purposes (see Processing for Journalistic Purposes).
- Processing for archiving in the public interest, scientific or historical research, or statistical purposes (see Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes).
- Processing for personal, family, or genealogical research or to maintain or publish family chronicles and biographies (see Processing for Personal, Family, or Genealogical Research or to Maintain or Publish Family Chronicles and Biographies).
- Secrecy obligations (see Secrecy Obligations).
- Processing in the employment context (see Processing in the Employment Context).

Processing for Journalistic Purposes

The GDPR permits EU member states to establish derogations from the GDPR when necessary to reconcile the right to personal data protection with the right to freedom of expression and information, including when processing for journalistic purposes or for academic, artistic, or literary expression (Article 85, GDPR). The Data Protection Act permits controllers to deny, limit, or delay providing data subjects access to their personal data under GDPR Article 15 when the controller plans to publish it in the editorial section of periodically published media and providing access would:

- Disclose the source of the information.
- Provide insight into drafts of publications.
- Threaten the free formation of public opinion.

(Article 25(1), Data Protection Act.)

Members of the press may also refuse, limit, or delay providing data subjects access to their personal data under GDPR Article 15 if they are processing the personal data exclusively as a work aid (Article 25(2), Data Protection Act).

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

The GDPR permits EU member states to establish rules when processing personal data for archiving in the public interest, scientific or historical research, and statistical purposes (Article 89, GDPR). The Data Protection Act permits processing personal data if necessary for archiving in the public interest, scientific or historical research, or statistical purposes if the following conditions apply:

- The data is publicly accessible.
- The data is pseudonymized and the controller cannot identify the data subject.
- Obtaining data subject consent is impossible or involves disproportionate effort because the data subject is not reachable.
- The controller takes appropriate and specific measures to safeguard the data subjects' interests under Data Protection Act Article 21(2).

(Articles 27(2) and 29(2), Data Protection Act.)

The Data Protection Act also permits processing special categories of personal data without data subject consent if:

- The processing is necessary for archiving in the public interest, scientific or historical research, or statistical purposes.
- The controller takes appropriate and specific measures to safeguard the data subjects' interests under Data Protection Act Article 21(2).
- The controller's interests outweigh the data subjects' legitimate interests in preventing the processing

in the case of processing for scientific or historical research or statistical purposes only.

(Articles 27(1) and 29(1), Data Protection Act; see Processing Special Categories of Personal Data.)

Data Protection Act Articles 27(1) and (2) and 29(1) and (2) also apply to personal data that the controller lawfully obtained for other purposes (Articles 27(3) and 29(3), Data Protection Act).

Controllers processing personal data for scientific or historical research or statistical purposes must:

- Anonymize the personal data as soon as the processing purpose allows, unless it conflicts with the data subject's legitimate interests.
- Separately store the characteristics that enable the controller to attribute personal or material circumstances to an identifiable individual.
- Only combine the separately stored information to the extent required by the processing purpose.
- Only publish the personal data with data subject consent or if the personal data is indispensable for presenting the research findings.

(Article 27(5), (6), Data Protection Act.)

The Data Protection Act permits controllers to restrict certain data subject rights when processing for archiving in the public interest, scientific or historical research, or statistical purposes. For more information on these restrictions, see Data Subject Rights Restrictions When Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes.

Processing for Personal, Family, or Genealogical Research or to Maintain or Publish Family Chronicles and Biographies

The Data Protection Act permits controllers to process personal data without data subject consent if required for personal, family, or genealogical research or to maintain or publish family chronicles and biographies. Controllers may also process special categories of data for these purposes if the processing is required and the controller's interests outweigh the data subject's interests in preventing the processing. Controllers must take appropriate and specific measures to safeguard the data subject's interests under Data Protection Act Article 21(2) when processing special categories of data for these purposes. (Article 28, Data Protection Act.)

Secrecy Obligations

The GDPR permits EU member states to adopt rules specifying the powers of supervisory authorities under GDPR Articles 58(1)(e) and (f) regarding controllers and processors that are subject to an obligation of professional secrecy or other equivalent secrecy obligation (Article 90, GDPR).

The Data Protection Act suspends the Data Protection Office's investigative powers under GDPR Articles 58(1)(e) and (f) if exercising these powers would violate secrecy obligations held by the persons set out in Section 121(1), (3), and (4) of the Liechtenstein Criminal Code or their processors. If the Data Protection Office obtains personal data subject to a professional secrecy obligation in the course of an investigation, it must also maintain that secrecy. (Article 30(3), Data Protection Act.)

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 Data Protection Act does not set out specific rules for personal data processing in the employment context. However, Section 1173a Article 28a(1) of the General Civil Code contains provisions generally permitting personal data processing in this context for specific reasons. The details of the General Civil Code are outside the scope of this Note.

Other GDPR Derogations

Processing Necessary for a Legal Obligation, Public Interest Purposes, or the Exercise of Official Authority

The GDPR permits EU member states to introduce more specific rules for processing necessary:

- To comply with a legal obligation (Article 6(1)(c), GDPR).
- To perform a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e), GDPR).

(Article 6(2), (3), GDPR.)

The Data Protection Act permits public bodies to process personal data if necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 4, Data Protection Act).

Prior Consultation and Authorization Requirements

The GDPR requires controllers to consult with the relevant supervisory authority before processing when

a data protection impact assessment under GDPR Article 35 indicates that the processing would result in a high risk to data subjects in the absence of measures to mitigate the risk (Article 36(1), GDPR). The GDPR permits EU member states to require controllers to consult with and obtain prior authorization from the relevant supervisory authority for certain processing carried out in the public interest, including processing relating to social protection and public health (Article 36(5), GDPR).

The Data Protection Act requires controllers to notify the Data Protection Office in writing and provide certain information before implementing video surveillance (see Video Surveillance). Controllers that received approval to conduct video surveillance under Liechtenstein's previous data protection law must complete the notification required under Data Protection Act Article 5(7) before the previous approval expires (Article 89, Data Protection Act).

Supervisory Authority

GDPR Article 54 requires each EU member state to establish a supervisory authority. The Data Protection Act establishes the *Datanschutzstelle* (Data Protection Office) as the national supervisory authority (Article 9, Data Protection Act). In addition to the tasks and powers specified in GDPR Articles 57 and 58, the Data Protection Act grants additional powers to the Data Protection Office, for example, the power to:

- Dispense with the controller's opportunity to comment on an alleged infringement under GDPR Article 58(2)(b) to (gg), (i), and (j) if an immediate decision is necessary due to imminent danger, public security or public interest reasons, or conflicts with a compelling public interest.
- File complaints against public and non-public bodies it believes have:
  - violated the Data Protection Act or other data protection legislation; or
  - deficiently processed personal data.
- Warn controllers that intended processing operations are likely to violate the Data Protection Act or other data protection legislation.
- Access all public and non-public entities' premises, data processing equipment and devices, and personal data necessary to perform its tasks after giving notice.
- Demand the dismissal of a DPO if the DPO does not have the expert knowledge needed to perform their tasks or has a serious conflict of interests under GDPR Article 38(6).

(Article 17(1), (2), (4), (6), Data Protection Act.)

Administrative Fines and Other Penalties for GDPR Violations

The Data Protection Act authorizes the Data Protection Office to impose administrative fines against any person who negligently violates the GDPR:

- Up to CHF11 million or, in case of legal entities, up to 2% of the previous year's total worldwide annual turnover, whichever is higher, for infringements under GDPR Article 83(4).
- Up to CHF22 million or, in case of legal entities, up to 4% of the previous year's total worldwide annual turnover, whichever is higher, for infringements under GDPR Article 83(5) and (6).

(Article 40(1), (2), Data Protection Act.)

The GDPR permits EU member states to specify penalties applicable to GDPR violations that are not subject to administrative fines under GDPR Article 83 (Article 84, GDPR). The Data Protection Act permits the district court to impose criminal penalties for violations, including:

- Up to six months' imprisonment or a fine up to 360 daily fine units for anyone who:
  - obtains non-public personal data without authorization; or
  - intentionally and without authorization makes accessible, discloses, or utilizes secret personal data obtained through their profession.
- Up to one year's imprisonment or a fine up to 360 daily fine units for anyone who makes accessible, discloses, or utilizes secret personal data obtained through their profession as set out above for a pecuniary benefit or to disadvantage another person.

(Articles 41 and 42, Data Protection Act.)

Any person who has suffered material or non-material damage from a violation of the GDPR or Data Protection Act Chapters I and II may receive compensation from the controller or processor for the damage suffered (Article 44, Data Protection Act).

For more on enforcement and sanctions under the GDPR, see Practice Note, Enforcement, Sanctions, and Remedies under the GDPR.

Administrative Fines for Public Authorities and Bodies

The GDPR permits EU member states to specify whether and to what extent supervisory authorities may impose administrative fines on public authorities and bodies (Article 83(7), GDPR). The Data Protection Act specifically exempts public authorities and bodies from administrative fines (Article 40(7), Data Protection Act).

Using Scoring and Credit Reports

The Data Protection Act permits controllers to use a probability value or score for a person's future actions when deciding whether to create, execute, or terminate a contractual relationship with that person only if:

- The controller complies with data protection law.
- The data the controller uses to calculate the probability value:
  - is demonstrably essential for doing so based on a scientifically recognized mathematic or statistical procedures; and
  - does not exclusively contain address data.
- The controller notifies the data subject in advance if it uses address data and documents the notification.

(Article 31(1), Data Protection Act.)

The Data Protection Act permits controllers to use a probability value calculated by a credit reporting agency to determine a person's ability and willingness to pay when including information on claims concerning non-performance and:

- The controller meets the requirements in Data Protection Act Article 31(1).
- The debtor's non-performance has been the subject of a writ of execution under Enforcement Act Article 1 (in German).
- The debtor's non-performance has been determined under Bankruptcy Act Article 66 (in German) and the debtor did not dispute it at the bankruptcy trial.
- The debtor:
  - has explicitly acknowledged their non-performance;
  - was notified at least twice in writing after the due date and at least four weeks have elapsed since the first reminder;
  - was previously notified of possible consideration by a credit reporting agency at least in the first reminder; and
  - has not disputed the claim.
- The controller can terminate the contractual relationship on which the claim is based without prior notice because of outstanding debts and notified the debtor that a credit reporting agency may use the information.

(Article 31(2), Data Protection Act.)

The rules set out in Data Protection Act Article 31(1) and (2) do not affect the lawfulness of processing other data relevant to creditworthiness, including probability values, under general data protection law (Article 31(3), Data Protection Act).

Video Surveillance

The Data Protection Act permits video surveillance of publicly accessible areas only:

- As far as necessary:
  - for public bodies to perform their tasks;
  - to determine who is allowed to access the area; or
  - to safeguard legitimate interests for specifically defined purposes.
- If nothing indicates that data subjects have overriding legitimate interests.

(Article 5(1), Data Protection Act.)

The protection of life, health, or freedom is a particularly important interest for those present in:

- Large publicly accessible facilities, such as sports facilities, entertainment venues, shopping centers, and parking lots.
- Vehicles and large public transport facilities.

(Article 5(2), Data Protection Act.)

Controllers operating a video surveillance system must:

- Inform the public as early as possible by appropriate measures:
  - that video surveillance is in operation; and
  - of their name and contact details.
- Only store or use the video surveillance data if:
  - necessary to achieve the collection purposes; and
  - the data subjects do not have an overriding legitimate interest.
- Only further process the data collected by video surveillance to the extent necessary to:
  - avert threats to state or public security;
  - avert serious danger to life, limb, freedom, or property; or
  - to prosecute criminal offenses or safeguard evidence.
- Inform data subjects under GDPR Articles 13 and 14 if it attributes data collected through video surveillance to them.
- Comply with GDPR Article 32 (Security of processing).
- Delete data collected through video surveillance immediately if:
  - the controller no longer needs it for the collection purpose; or
  - the data subject's legitimate interests prevent continued retention.

- Notify the Data Protection Office in writing before implementing video surveillance with the following information:
  - the controller's name, contact information, responsible person, place of business, and establishment;
  - the type of video surveillance, for example, recording, live, fixed mounted, pan and tilt, or video and audio;
  - the monitored areas;
  - the hours of operation;
  - the purpose and necessity of the video surveillance and data processing;
  - the proportionality of the processing, such as less intrusive measures and data subjects' legitimate interests;
  - the monitored persons;
  - a description of the data processing, such as technical procedures and data transfers;
  - data storage details, such as the modalities, duration, and erasure of data; and
  - how it will inform data subjects of the video surveillance.

(Article 5(3) to (7), Data Protection Act; Article 5, Data Protection Regulation.)

Data Protection Act and GDPR Statutory References

Subject Matter	Data Protection Act Article	GDPR Article(s) Permitting Member State Derogation
Applicability of Liechtenstein law (see Applicability of the GDPR and Liechtensteinian Law)	2	N/A
Appointing a data protection officer (see Data Protection Officers)	38	37(4), 38(5)
Processing special categories of personal data (see Processing Special Categories of Personal Data)	21	9(2)(b), (g), (h), (i), (j)
Processing criminal conviction and offense data (see Processing Criminal Conviction and Offense Data)	n/a	10
Processing for secondary purposes (see Processing for Secondary Purposes)	23	6(4)
Age of child consent (see Child Consent)	N/A	8(1)
Data subjects' rights (see Data Subjects' Rights and Data Protection Act Variations to Data Subject Rights)	30, 32 to 37	23, 85, 89
Processing for journalistic purposes (see Processing for Journalistic Purposes)	25	85

Liechtensteinian Implementation of the GDPR

Subject Matter	Data Protection Act Article	GDPR Article(s) Permitting Member State Derogation
Processing for archiving in the public interest, scientific or historical research, or statistical purposes (see Processing for Archiving in the Public Interest, Scientific or Historical Research, or Statistical Purposes)	27, 29	89(2), (3)
Processing for personal, family, or genealogical research or family chronicles and biographies (see Processing for Personal, Family, or Genealogical Research or to Maintain or Publish Family Chronicles and Biographies)	28	N/A
Secrecy obligations (see Secrecy Obligations)	30(3)	90
Processing employee personal data (see Processing in the Employment Context)	Civil Code § 1173a Article 28a(1)	88
Processing necessary for a legal obligation, public interest purpose, or to exercise official authority (see Processing Necessary for a Legal Obligation, Public Interest Purposes, or the Exercise of Official Authority)	4	6(1)(c), (e)
Using Scoring and Credit Reports (see Using Scoring and Credit Reports)	31	N/A
Prior consultation and authorization requirements (see Prior Consultation and Authorization Requirements)	89	36(5)
Supervisory authority (see Supervisory Authority)	9 to 17	54
Administrative fines and additional penalties for GDPR violations (see Administrative Fines and Other Penalties for GDPR Violations)	40 to 42, 44	84
Public authorities and bodies (see Administrative Fines for Public Authorities and Bodies)	40(7)	83(7)

Subject Matter	Data Protection Act Article	GDPR Article(s) Permitting Member State Derogation
Video surveillance (see Video Surveillance)	5 Data Protection Regulation Article 5	6(2)