European Law Institute Data Protection Report

The ELI is committed to reviewing its data policies regularly and is grateful to be notified of any potential ways of improving them.

Introduction

Legislative Framework

The General Data Protection Regulation (GDPR), which applies from 25 May 2018, will establish a new set of data protection provisions applicable across the European Union. As mentioned in its article 1(1), the regime lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

The regulation applies inter alia if a data controller (an organisation that collects data from EU residents), processor (an organisation that collections, records, storages personal data on behalf of a controller) or the data subject (person) is based in the EU. It therefore applies to the European Law Institute (ELI). Under the GDPR, the ELI's 'main establishment', namely the place of its central administration, is Vienna, Austria. By virtue of article 56, it is the Austrian supervisory authority that has jurisdiction under the Regulation and Austrian data protection laws apply to the extent permitted under the GDPR. The relevant authority for the enforcement of privacy and data protection laws in Austria is the Data Protection Agency. The ELI will naturally cooperate with the Data Protection Agency at all times (article 31 GDPR).

In Austria, the Data Protection Act 2000 currently governs the collection, storage and usage of personal data. The Act is based on the EU Data Protection Directive (95/46/EC). In June 2017, the Data Protection Act 2018 implementing the EU GDPR was adopted by the Austrian legislature. The Act became applicable on 25 May 2018. Overall, the national implementation Act of 2018 is quite minimalistic and just uses a limited number of the possibilities offered by the Regulation to implement more stringent or deviating provisions.

This guide has been drafted to aid the ELI in complying with its obligations under the GDPR. The ELI must implement necessary measures to ensure and be able to demonstrate that processing is performed in accordance with the Regulation (articles 24 and 25). It is also essential that those measures are periodically reviewed and updated (article 24).

Principles Relating to Processing of Personal Data

The ELI needs to ensure, in accordance with article 5 of the GDPR, that personal data is processed lawfully. More specifically, it must be processed:

- fairly and in a transparent manner in relation to the data subjects
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, is erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- processed in a manner that ensures appropriate security of the personal data

As a controller, the ELI is responsible for and must be able to demonstrate compliance with article 5.

Type of Data

Processing of data is lawful only if, and to the extent that, at least one of several points under artide 6 GDPR applies. The ELI controls and processes personal data of various groups of individuals including (prospective) ELI members, (prospective) project contributors, (prospective) employees, (prospective) event attendees, newsletter recipients (including ones that are not ELI members) as well as persons that contact the ELI on an *ad hoc* basis or vice versa. For further details, please consult the table below.

Category of Data Processed	Members	Project Contributors	Employees	Event Attendees (Externals)	Newsletter Recipients (Externals)	Ad Hoc Contacts (Externals)
Title	✓	✓	✓	✓		✓
Name	✓	✓	✓	✓	✓	✓
Surname	✓	✓	✓	✓	✓	✓
Date of Birth/Age	✓		✓			
Nationality	✓	✓	✓			✓
Gender	✓		✓	✓		
Family Status			✓			
Languages Spoken	✓		✓			
Belief System			✓			
Physical Address	✓	✓	✓	✓		✓
E-mail Address	✓	✓	✓	✓	✓	✓
Website	✓	✓	✓			✓
Telephone No	✓	✓	✓	✓		✓
Mobile No	✓	✓	✓	✓		✓
Fax	✓	✓				✓
ID	✓[1]		✓			
Signature	✓[2]	✓	✓			✓
Social Security No			✓			
Voice	✓[3]	✓	✓	✓		
Video Recordings	✓	✓	✓	✓		
Image	✓[4]	✓	✓	✓		
Health Insurance Details			✓			
Dietary Requirements	✓	✓	✓	✓		
Special Needs	✓[5]		✓	✓		
Occupational Details	✓	✓	✓	✓		
Occupational Interests	✓	✓	✓	✓		
Next of Kin Details			✓			
Bank Details	✓	✓	✓	✓		
Criminal Record Declaration			✓			
CV	✓	✓	✓	✓		
Proof of Qualifications/Certificates			✓			
Performance Records			✓			

[1] In the case some members, eg Executive Committee members.
[2] In the case some members, eg Executive Committee members.
[3] In the case of some conferences or meetings.
[4] Mainly in the case of members of key ELI bodies or for PR related activities.
[5] Mainly in the case of event attendance.

Sensitive Data (articles 9 and 10)

Apart from data on one's belief system, which is required by Grant Thornton for payroll purposes, and data concerning health, the ELI does not process any special categories of personal data under articles 9 or 10 GDPR. The exemption under article 9(2)(b) on the processing of data necessary in the field of employment and social security applies to justify the processing of the above type of data.

Lawfulness of Processing (Article 6)

The processing of all the above data is lawful on the basis that:

- the data subject has given consent to the processing of his or her personal data for one or more specific purposes (article 6(a)) – prospective ELI members, project contributors, employees as well as (prospective) event attendees and newsletter recipients that are not ELI members
- processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract (article 6(b)) – current ELI members; employees
- processing is necessary for compliance with a legal obligation to which the controller is subject (article 6(c)) – all of the above to the extent necessary for EU, tax, social security reporting, etc, purposes
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (article 6(f)) – ad hoc correspondences

Rights of the Data Subject

Facilitating the Exercise of the Rights of the Data Subject (Article 12)

In accordance with article 12(3) GDPR, the ELI will provide the information requested by a data subject in the exercise of his or her rights below without undue delay and in any event within in one month (or two months, taking into account the complexity and number of requests) of receipt of the request. In the latter case, the data subject will be informed of any extensions, together with reasons for the delay. Note that article 12 applies to a broad range of articles includes articles 15–22.

If the ELI does not take action on the request of the data subject, the ELI will give the data subject, within one month of the request, reasons for not taking action and the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy (article 12(4) GDPR).

The ELI is only obliged to comply to the extent that a request is not manifestly unfounded nor excessive and will reserve the right to charge a reasonable fee in the case of repetitive requests or refuse to act on the request (article 12(5) GDPR).

Right to Withdraw Consent (Article 7)

As is required under article 7 GDPR, the ELI seeks written consent for the collection and processing of data relevant to the above groups. In accordance with article 7(3) GDPR, the withdrawal of consent does not, however, affect the lawfulness of processing based on consent before its withdrawal.

Declarations of consent are presented to data subjects prior to consent being given, in a manner consistent with article 7(2) GDPR so that data subjects have intelligible and easily accessible information on the purpose and reasons for which their data is collected and processed.

The right to withdraw consent at any time, as is required under article 7(3) GDPR, is also included in written declarations.

Information to be Provided on the Collection of Data from Data Subject (Article 13)

The ELI includes the following when data is obtained from data subjects:

- the ELI's identity and contact details
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- the recipients or categories of recipients of the personal data, if any
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability
- where the processing is based on point (f) of article 6(1), the legitimate interests pursued by the controller or by a third party
- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- the right to lodge a complaint with a supervisory authority
- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data

The ELI does not exercise automated decision-making.

In the rare case that the ELI has to process personal data for a purpose other than that for which the personal data was collected, the ELI will provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to above.

Information to be Provided on the Collection of Data from Non-Data Subject (Article 14)

Where personal data has not been obtained from the data subject, the ELI will provide the data subject with the following information:

- the identity and the contact details of the controller and, where applicable, of the controller's representative
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing
- the categories of personal data concerned
- the recipients or categories of recipients of the personal data, if any
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period

- where the processing is based on point (f) of article 6(1), the legitimate interests pursued by the controller or by a third party
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability
- the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal
- the right to lodge a complaint with a supervisory authority
- from which source the personal data originated, and if applicable, whether it came from publicly accessible sources

Right of Access to Personal Information (Article 15)

By article 15, the ELI's data subjects have the right to seek confirmation from the ELI as to whether or not personal data concerning them is being processed. They are also entitled to access to the personal data and information including:

- the purposes of the processing
- the categories of personal data concerned
- the recipients or categories of recipient to whom the personal data has been or will be disclosed
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period
- the existence of the right to request from the ELI rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing
- the right to lodge a complaint with a supervisory authority
- where the personal data is not collected from the data subject, any available information as to their source

The data subject is also entitled to obtain a copy of the personal data undergoing processing.

Right to Rectification (Article 16)

The ELI will ensure the rectification or completion of inaccurate personal data concerning data subjects following a request by them. It will make best efforts to communicate the foregoing to any recipients of the personal data of the subject and if requested, will inform the data subject accordingly, of having done so (article 19 GDPR).

Right of Erasure (Article 17)

The ELI will ensure, in accordance with article 17 GDPR, that data subjects have the right to request erasure of personal data related to them without undue delay on any one of a number of grounds, including where:

- the personal data is no longer necessary in relation to the purposes for which they were collected or otherwise processed
- the data subject withdraws consent on which the processing is based
- the personal data have been unlawfully processed
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject

Where personal data is made public, the ELI will take appropriate steps to inform processors of the data subject's request for erasure in line with (article 17(2) GDPR)).

The ELI will not erase data to the extent that processing is necessary:

- for exercising the right of freedom of expression and information
- for compliance with a legal obligation requires processing by Union or Member State law to which the ELI is subject
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing
- for the establishment, exercise or defence of legal claims

The ELI will make best efforts to communicate the erasure to any recipients of the personal data of the subject and if requested, will inform the data subject accordingly, of having done so (article 19 GDPR).

Right to Restriction of Processing (Article 18)

The ELI will restrict processing where one of the data subject requests this on the following grounds:

- the accuracy of the personal data is contested, for a period enabling the ELI to verify the accuracy of the personal data
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of its use instead
- the ELI no longer needs the personal data for the purposes of the processing, but is required by the data subject for the establishment, exercise or defence of legal claims

The ELI will make best efforts to communicate the restriction of processing to any recipients of the personal data of the subject and if requested, will inform the data subject accordingly, of having done so (article 19 GDPR).

Data Portability (Article 20)

The ELI will facilitate data portability in accordance with article 20 GDPR.

General Obligations of the ELI as a Controller and Processor of Personal Data

Transferring Personal Data (Article 28)

Where processing is to be carried out on behalf of the ELI, a contract will be entered into giving prior specific or general written authorisation by the ELI.

Amongst other things, the contract sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller, in addition to other points mentioned in article 28(3).

Records of Processing Activities (Article 30)

The ELI records data categories under the University of Vienna's *Verarbeitungsverzeichnis* catalogue. This has already been done.

Security of Processing (Article 32)

The ELI will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. By entering into confidentiality agreements with staff members and other individuals that deal with the ELI with access to personal and other important data, the ELI can ensure the confidentiality of processing systems and services.

With servers operated by the University of Vienna, the ELI can ensure restoration of personal data in a timely manner in the event of a physical or technical incident. It will embark on regularly testing, assessing and evaluating of the effectiveness of technical and organisational measures for ensuring the security of the processing.

Data Protection Officer (Article 37)

The ELI does not fall within any of the categories in article 37 warranting the designation of a data protection officer.

Transfer of Data to Third Countries or International Organisations (Articles 44–50)

The ELI needs to ensure that any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation take place subject to the provisions of the GDPR. All provisions in Chapter Five of the GDPR shall be applied in order to ensure that the level of protection of natural persons guaranteed by the Regulation is not undermined. This is the case for example with the ELI's current project on Principles for a Data Economy. The ELI will have to demonstrate that the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request or that it is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person (see articles 49(1)(b and (c).

Fines (Article 83)

Infringement provisions under the GDPR are subject, among other sanctions, to administrative fines of up to €20 million, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. The Data Protection Act 2018 also provides an administrative penalty of up to €50,000, applicable to less serious infringements of data protection provisions not contained in the Regulation but contained in the Act.

Notification of Data Breaches

Under the GDPR, data controllers are required to notify any affected data subjects and/or supervisory authorities without undue delay of any data breaches.

Notification of a Personal Data Breach to the Supervisory Authority (Article 33)

The ELI must notify its supervisory authority, the Austrian Data Protection Agency, without undue delay, and in any case within a period of 72 hours after becoming aware of the data breach about that breach, *unless the breach is unlikely to result in a risk to the rights and freedoms of the individuals*. The notification will at least:

- describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained
- describe the likely consequences of the personal data breach
- describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects

Notification of a Personal Data Breach to the Data Subject (Article 34)

Individuals must be notified of a data breach by the ELI, without undue delay where the breach is likely to result in a high risk to the rights and freedoms of natural persons. However, the notification of data subjects is not required if:

- the data controller has implemented appropriate technical and organisational protection measures that render the personal data unintelligible to any person who is not authorised to access it, such as encryption
- the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise
- it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner