Policy Name:	***Data Protection Policy***
Policy Ref:	POL/PV/DP/CC/0008F
Who it applies to:	Employees, Volunteers, Directors, Board Members, Trustees, Members and/or other Associated Persons.
Date of Issue:	March 2019
Last Revision Date:	July 2021
Review Date:	January 2023
Version:	1.8
Policy Type:	Corporate
Policy Owner:	Corporate Compliance Manager/ Group Privacy Officer
Approved By:	Corporate Policy Review Panel (CPRP)
Equality Impact Assessment Screened	Yes
Contractual terms and conditions, which will be changed following legal requirements.	No
Company Policy relates to:	Group

Data Protection Policy

Data Protection Policy

Contents

Introduction

This Policy forms part of the Chartered Institute of Legal Executives' (CILEX) internal control and corporate governance arrangements. CILEX means here the Chartered Institute of Legal Executives and its subsidiaries.

The CILEX Board is committed to ensuring that effective policies operate throughout CILEX.

This policy is not contractual, but it is intended as a statement of current CILEX strategy and its commitment to operate a fair procedure, considering statutory and other guidelines. CILEX, therefore reserves the right to amend this policy and procedure as necessary to meet any changing requirements.

Everyone has statutory rights with regards to how their personal information is handled. CILEX is required to keep certain information on its employees, members, service users, volunteers and other stakeholders to carry on its day-to-day operations and to comply with legal obligations.

This policy explains CILEX's underlying approach to its Data Protection compliance, documents the roles and responsibilities and outlines the key aspects of the Data Protection Management Process with identifying the main reporting procedures. The Data Protection GDPR Procedure, which expands upon this policy should be referred to for additional information.

Purpose and Scope of the Policy

This policy sets out the framework by which personal data is processed, handled, stored and disposed of within CILEX, in line with the current UK Data Protection legislation and how individuals (known as Data Subjects) are permitted to access their personal data held by CILEX. CILEX is made up of the following organisations:

- Chartered Institute of Legal Executives (CILEX)
- CILEX Foundation
- CILEX Law School

CILEX has adopted the following principles, in accordance with the UK Data Protection legislation to govern its collection, use, retention, transfer, disclosure and destruction of Personal Data:

Principle 1: Lawfulness, Fairness and Transparency

Personal Data shall be processed lawfully, fairly and in a transparent manner, in relation to the Data Subject.

This means that CILEX must tell the Data Subject what processing will occur (transparency); the processing must match the description given to the Data Subject (fairness) and it must be for one of the purposes specified in the applicable UK Data Protection legislation (lawfulness).

Principle 2: Purpose Limitation

Personal Data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

This means that CILEX must specify exactly what the Personal Data collected will be used for and limit the processing of that Personal Data to only what is necessary to meet the specified purpose.

Principle 3: Data Minimisation

Personal Data shall be adequate, relevant and limited to what is necessary, in relation to the purposes for which they are processed.

This means that CILEX must not store any Personal Data beyond what is strictly required.

Principle 4: Accuracy

Personal Data shall be accurate and where necessary kept up-to-date. Every reasonable step must be taken to ensure that personal data is inaccurate is either erased or rectified without delay.

This means that CILEX must have in place processes to check the accuracy of the data it collects and processes to keep the data updated, as necessary.

Principle 5: Storage Limitation

Personal Data shall be 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.

This means that CILEX must, wherever possible, store Personal Data in a way that limits or prevents identification of the Data Subject.

Personal data must not be kept for longer than CILEX requires it.

The information that CILEX retains, the reasons for storing it and the retention periods are established in the GDPR Data Audit/DPIA Spreadsheet. The retention periods of our documentation are set out in our Archive, Retention and Destruction Procedure.

Principle 6: Integrity, Confidentiality & Security

Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

This means that CILEX must use appropriate technical and organisational measures to ensure the integrity and confidentiality of Personal Data are maintained at all times.

Principle 7: Accountability

The Data Controller and the Data Processor shall be responsible for and be able to demonstrate compliance with the relevant UK Data Protection legislation.

This means that CILEX must demonstrate that the Data Protection Principles (outlined above) are met for all Personal Data for which it is responsible.
As necessary, the GDPR Data Audit/DPIA form will be completed for new processes and major projects. These will be reviewed regularly and when there is a change to the nature, scope, context or purpose of processing.

CILEX will respect the following Rights for the Individuals, in accordance with the UK Data Protection legislation:

Right 1: The Right to be Informed

Individuals have the right to be informed about the collection, sharing, protection and use of their personal data.

Right 2. The Right of Access

Individuals have the right to request access their personal data that we hold.

Right 3. The Right to Rectification

Individuals have a right to have inaccurate personal data rectified, removed or completed if it is incomplete. If the personal data is found to be incorrect, but is unable to be updated, this should be removed.

Right 4. The Right to Erasure

Under certain circumstances, a data subject may request for us to delete their information that we retain regarding them, with the exception of any information that we are legally required to retain and for the other exemptions set out in UK Data Protection legislation (Your right to get your data deleted | ICO).

Right 5. The Right to Restrict Processing

Individuals have the right to request the restriction or suppression of their personal data, in certain circumstances.

Right 6. The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services, which should be provided in such a way that information can be copied or transferred from one IT environment safely and securely without affecting its usability.

Right 7. The Right to Object

Individuals have the right to object to the processing of their personal data, in certain circumstances. For example, individuals have an absolute right to stop their data being used for direct marketing.

Right 8. Rights Concerning Automated Decision-Making and Profiling

CILEX may carry out this type of decision making where the decision is either A) necessary for the entry into or performance, B) authorised by Union or Member State Law applicable to the Data Controller or based on the individual's explicit consent.

If CILEX carries out automated decision-making and profiling, it needs to ensure that it has a lawful basis to carry out the profiling and/or automated decision-making and document this in its Data Protection Policy.

When using CILEX online membership application forms, an automated decision is made to allocate the person to the appropriate Membership Grade.

CILEX performs automated decision-making at the beginning of the refresher training modules on the Learning Hub to assess the employee's knowledge about specifics topics.

CILEX makes automated decision-making for tutors' management to allocate students to tutors.

CILEX has determined the lawful basis to carry out the automated decision-making. The lawful basis for CILEX to carry out automated decision-making for the membership registration is Consent of the Data Subject and for the tutor management and the Learning Hub it is Legitimate Interest and Employment Law.

For more information about how to exercise any of the individual's right under UK Data Protection legislation see Appendix A.

Definitions

Personal Data: Any information relating to an identified or identifiable natural person (Data Subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location of data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Special Categories of Personal Data: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and processing of genetic data, biometric data for this purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sexual orientation.

Data Controller: The natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of processing the personal data.

Data Subject: Any living individual, who is the subject of personal data held by an organisation.

Processing: Any operation or set of operations, which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording,

organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available alignment or combination, restriction, erasure or destruction.

Profiling: It is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour. This definition is linked to the right of the Data Subject to object to the profiling and a right to be informed about the existence of profiling, of measures based on profiling and a right to be informed about the existence of profiling and the envisaged effects of profiling on the individual.

Personal Data Breach: A breach of security leading to the accidental or unlawful, destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed. There is an obligation on the Data Controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data Subject Consent: This means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Child: The GDPR defines a child as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. The processing of personal data of a child is only lawful if parental or custodian consent has been given or authorised by the holder of parental responsibility over the child.

Third Party: A natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, Data Processor and persons who under the direct authority of the Data Controller or Data Processor are authorised to process personal data.

Filing System: Any structured set of personal data, which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Responsibilities

It is the responsibility of all employees to ensure that the principles of UK Data Protection legislation are adhered to.

It is the responsibility of the Corporate Compliance Manager (CILEX) to ensure that this policy and the associated procedure document are reviewed and updated where necessary.

The Corporate Compliance Manager is also the Group Privacy Officer (Email: privacyofficer@cilex.org.uk).

Legal Obligations

The statutory and/or regulatory directives and legislation on which this Policy is based upon is the current UK Data Protection legislation.

This is all applicable UK Data Protection and Privacy legislation in force from time-to-time, including the General Data Protection Regulation (EU) 2016/679, the UK Data Protection Act 2018 and the Privacy and Electronic Communications (EU Directive) Regulations 2003 (as amended) (PECR) and any superseding legislation and all other applicable laws, regulations, statutory instruments and/or any codes, practice or guidelines issued by the relevant data protection or supervisory authority in force from time to time and applicable to a Party, relating to the processing of personal data and/or governing individual's rights to privacy.

From 28th June 2021, the UK has been granted an adequacy decision by the EU, which covers data transfers between the UK and the EU and this adequacy decision is due to be reviewed in four years' time (on 28th June 2025) with a view to this safeguard remaining in place for UK/EU Data Transfers.

Relevant Policy References

The following CILEX Group Corporate policies fall within the reach of this policy:

- Archive, Retention and Destruction Policy
- Information Security Policy
- Privacy Policy
- Cookies Policy
- Customer Service Standards
- Corporate Complaints Policy
- Redaction Policy
- Appointment of Consultants Policy
- Conflict of Interest Policy
- Fraud Policy
- Potential Data Security Incident Reporting Policy
- Publication of Documents Policy
- Safeguarding Policy
- Recruitment Policy
- Whistleblowing Policy, as well as other policies not listed here.

Competence

In accordance with the accepted principles of good governance, it is essential that the required capabilities of members of the CILEX Board (and its committees) are developed and maintained. Board Members must therefore ensure that they understand their obligations, with regard to UK Data Protection and to seek and be given the necessary training and support to enable them to fulfil those obligations.

It is also necessary for all employees to understand fully their roles, responsibilities and accountabilities, thus requiring them to maintain an up-to-date knowledge of UK Data Protection and how it is managed by CILEX.

All new starters are required to undertake an online training course in the principles of UK Data Protection. Also, refresher training is carried out yearly within the Data Protection e-Learning module. The Learning and Development Team within the Human Resources Directorate are responsible for arranging the online compliance training.

Miscellaneous

Potential Data Security Incident (PDSI)
When the Group Privacy Officer has been made aware of a Potential Data Security Incident (PDSI) (also commonly known as a data security breach), a risk assessment will be carried out by the Corporate Compliance Team (and any other persons that will be considered necessary). If the risk has been rated as High, the Group Privacy Officer will initiate a Data Security Incident Reporting Assessment Team (DSIBRAT) meeting. This will be completed within 72 hours.

CILEX manages its Potential Data Security Incidents (PDSI) via the Potential Data Security Incidents Reporting Policy.

External Privacy Notices

Where personal data is collected about an individual, they will be made aware of the purpose for which the data is collected and what it will be used for.

Each external website provided by CILEX will include an online 'Privacy Notice' and an online 'Cookie Notice' fulfilling the requirements of the law. See the Group Privacy Policy and Cookies Policy.

Information Commissioner's Office

In the United Kingdom, the Regulator is The Information Commissioner's Office:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel No: 0303 123 1113 (local rate) or 01625 545 745 (national rate)

Website: www.ico.org.uk

Appendix A: Data Protection – Query & Request

Following to individual's rights detailed in the Purpose and Scope of the Policy section above, individuals should be aware that CILEX can refuse to comply with a request, if it is manifestly unfounded or excessive. In order to decide if a request is manifestly unfounded or excessive, CILEX must consider each request on a case-by-case basis.

Due to COVID 19 restrictions we may have some difficulties locating individual's personal information retained in hard copies and stored in our offices in Kempston. However, we will make reasonable efforts to provide this information as part of your request, when necessary.

For more information about how we collect and use your data, please refer to our Privacy Statement.

If individuals have any questions about how CILEX process their personal data or would like to exercise any of their rights under the UK Data Protection legislation, they should log in to MYCILEX Portal and go to Contact Us, then select 'Data Protection: Query and Request' on 'My Query Relates to' section. If they do not have access to the MYCILEX Portal, or do not wish to log their details on the system, they can contact us by email at privacyofficer@cilex.org.uk.

The Right to be Informed

As part of a Data Subject Request, we will inform the individuals how their personal information is being used, who it is being shared with, the lawful basis in which we rely on to process their personal data, how it is protected, among others.

The Right of Access

As part of a Data Subject Access Request, CILEX may provide copies of the following information:

- **Customer Relationship Management (CRM) system:** the data that CILEX holds primarily relates to the individuals' contact details, employer details, subscriptions, examinations, qualification, assessments, and correspondence the individuals have had with CILEX.

- **Emails**: All those emails that the individuals have exchanged with anyone within CILEX. We will submit those emails that include their personal data[1].

[1] According to the Information Commissioners Office (ICO), just because an email contains individuals' name, it does not necessarily mean that contain personal data. The Data Protection regulation states that we should take into account the information we are processing together with all the means reasonably likely to be used by either us or any other person to identify the individual. Even if an individual is identified or identifiable, directly, or indirectly, from the data we are processing, it is not personal data unless it 'relates to' the individual. When considering whether information 'relates to' an individual, we need to consider a range of factors, including the content of the information, the purpose, or purposes for which we are processing it and the likely impact or effect of that processing on the individual.

- **Financial information**: invoices and payments details stored will be submitted.

- **CILEX Law School (CLS):** if individuals are or were a CLS learner/apprentice, CLS may have stored information about purchases of courses, study materials and the recordings of the webinars they attended to, etc. All this information could be provided as part of the request.

  CILEX will also provide requester's personal information stored in any of the systems used by CLS, such the CLS Hub.

- **CILEX Awarding Body**: if the individual is registered for CILEX qualification or exam, we may provide as part of the request (when applicable) any exam and/or assessment results, results notifications, centre result notifications, certificates and/or diplomas stored, exam scripts/assessment works, results notifications, among some other information.

- **Membership**: the membership database comprises personal details (main), membership applications, employment, home addresses, balances, finance, subscriptions, education details, committees, and classifications, contact history, events, advisor information, exemptions, and verifier, etc. CILEX may provide copies of the screens with the data we held about the individuals.

  The data that CILEX holds is taken and held for the purposes of maintaining membership records, ensuring that subscription requests are sent out to members, recording payments, and maintaining education and examination records of our members.

- **DotDigital**: the majority of general communications are sent from our mailing/communications system (DotDigital) so, personal data (name and email address) is also stored on this system. Screenshots from this system may also be provided as part of the request.

- **Human Resources**: if the individual works/worked for CILEX, we will provide as part of the request all the information in our libraries regarding contact details, payment specifications, childcare information, education details, absences, holidays, grievances, health issues, etc.

- **CILEX Regulation (CRL):** we will contact CRL to confirm whether they hold personal data from the requester. If so, this information will be also included as part of the request.

In general, CILEX only retains personal data for as long as necessary to fulfil the purposes for which it is being processed (including to comply with relevant legal or regulatory requirements,

and/or to resolve legal disputes). Personal information will be provided if it has not been confidentially disposed in accordance with the CILEX Archive, Retention and Deletion Policy.

That length of time for retention may vary depending on the reasons for which we are processing the personal data and whether we have a legal (for example under financial regulations) or contractual obligation to keep it for a certain amount of time.

All the documents provided will be appropriately redacted and where a document is more than a page long, CILEX will only provide redacted copies of the pages where search criteria is relevant.

Due to COVID 19 restrictions we may have some difficulties by locating your personal information retained in hard copies and stored in our offices in Kempston. However, we will make proportional efforts to provide this information as part of your request, when necessary.

The Right to Rectification

If a rectification request is received or identified, the Group Privacy Officer will check if the individual's data is inaccurate or incomplete, taking into account the information and evidence provided by the individual.

If the check confirms that the data is inaccurate, the Group Privacy Officer will take whatever steps are needed to rectify the data, involving any CILEX employees in the process.

Examples of common errors to personal data include but are not restricted to:

- Name is misspelt;
- Address is incorrect; such as the wrong flat or house number, wrong postcode, wrong street name, town, or city;
- Date of birth has the wrong day, month, or year;
- Details about education or employment are incorrect or have information missing;
- Errors on financial records.

When sending a request, the requester should include:

- Why they believe the data is inaccurate or incomplete;
- Explain how the data should be corrected;
- If necessary, provide evidence of the inaccuracies.

However, personal information can be also changed via the MYCILEX Portal.

The Right to Erasure

The erasure of an individual's personal data from all our data bases comprises the following:

1. **Customer Relationship Management (CRM) system**: CILEX will deactivate the requester's account and erase their personal data from our system if this is possible to do so. However, their personal data cannot be fully deleted in the following instances: CILEX Law School (CLS) has recorded a course and qualification registered on the system (see point 2); the Awarding Body has records of exams and assessments, certificates and

diplomas, exam scripts/scripts words (see point 8); and information which is part of their membership (see point 4).

2. **CILEX Law School (CLS):** if an individual has CLS Courses and Qualifications records, some of their personal data will remain stored in our records and libraries.

3. **CLS Hub:** this is the system used by CLS to deliver training/teaching to learners. The individuals will need to choose one of the following options:
    - delete all data;
    - anonymise their user profile;
    - suspend their accounts (they cannot log in, but any activity data still exists, and their accounts can be reactivated).

4. **Membership:** we cannot delete the information that the individuals provided to us when they joined as a CILEX member. This information may contain their membership and qualifications information.

5. **Other files and libraries:** the individual's request will be saved in our 'Other Rights Log' for compliance purposes[2].

6. **Invoices:** we are required by statute to retain records of financial transactions for at least 6 years.

7. **Emails**: we are not able to specifically delete the emails we have sent to and received from the individual. This information will be systematically deleted in accordance with our Archive, Retention and Deletion Policy.

8. **CILEX Awarding Body:** if we delete information about exams and assessments, certificates and diplomas, exam scripts/scripts words, etc, we will not be able to verify unit achievements or provide replacement results notifications. In this scenario, we will require confirmation that the individual understands the implications of the request. We will review the request on a case-by-case basis.

9. **CILEX Regulation (CRL):** depending on the type of information CRL retains about the individual, CRL will evaluate the request carefully and they will explain whether the personal information can be deleted.

10. **Mailing/communications system (DotDigital):** if the requester's personal data is registered in our DotDigital address book, their record will be deleted from the system.

[2] The personal data added to this log just includes full name and email address.

Additionally, as the record will be deleted from CRM (see point 1), the email address will not be held in our communication system any further. We will also add the individual's details to the suppression list so they should not get any further communications from us.

11. **RingCentral:** this is our cloud-based unified communications service that maintains records of calls with customers. If we find the individual's personal information recorded on RingCentral linked to the phone number on the requester's CRM record, we will delete the recordings.

12. **Backup's systems**: please note that we have weekly, monthly, and yearly tapes that will hold data for up to two years, but we are unable to selectively delete files from those. However, the data is not processed, and it would only be accessible by our system administrators and restored in the case of an emergency.

Due to COVID 19 restrictions we may have some difficulties by locating your personal information retained in hard copies and stored in our offices in Kempston. However, we will make proportional efforts to provide this information as part of your request, when necessary.

The Right to Restrict Processing

Individuals have the right to restrict the processing of their personal data if:

- where the individual contests the accuracy of their personal data and CILEX is verifying the accuracy of the data;
- the data has been unlawfully processed and the individual opposes erasure and requests restriction instead;
- CILEX no longer needs the personal data, but the individual asks CILEX to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to CILEX's processing their data under the right to object, and CILEX is considering whether its legitimate grounds override those of the individual.

If it is decided that the individual has the right to restrict processing their personal data, the Group Privacy Officer will take whatever steps are needed to restrict personal data. The Group Privacy Officer will take into account the following methods:

- temporarily moving the data to another processing system;
- making the data unavailable to users; or
- temporarily removing published data from a website.

If CILEx has disclosed the personal data to others, the relevant department must contact each recipient and inform them of the restriction of the personal data, unless this proves impossible or involves disproportionate effort.

The Right to Data Portability

Individuals may request a copy of their data for reuse across different services, which should be provided in a way so that information can be copied or transferred from one IT environment to another safely and securely without affecting tis usability.

The Group Privacy Officer will investigate if the data subject right to data portability applies or not. The right to data portability only applies when:

- CILEX's lawful basis for processing the information is consent or for the performance of a contract; and
- CILEX is carrying out the processing by automated means (i.e., excluding paper files).

If it is decided that the individual has the right to portability request, the Group Privacy Officer will take whatever steps are needed to entitle the individual to:

- receive a copy of their personal data; and/or
- have their personal data transmitted from CILEX to another controller.

CILEX should provide the personal data in a format that is structured, commonly used and machine-readable.

The Right to Object

The Group Privacy Officer will investigate if the data subject's right to object applies or not.

Individuals have the right to object to the processing of their personal data if it is for direct marketing purposes. If CILEX receives an objection to processing for direct marketing, CILEX must stop processing the individual's data for this purpose.

Individuals can also object if the processing is for:

- a task carried out in the public interest;
- the exercise of official authority vested in CILEX; or
- CILEX's legitimate interests.

In these circumstances, the right to object is not absolute. CILEX can continue processing if:

- CILEX can demonstrate compelling legitimate grounds for the processing, which override the interests, rights, and freedoms of the individual; or
- the processing is for the establishment, exercise, or defence of legal claims.

If CILEX is satisfied that it does not need to stop processing the personal data, the Group Privacy Officer will let the individual know, and explaining the decisions, informing the individual that they have the right to make a complaint to the ICO.

Rights Concerning Automated Decision Making and Profiling

We may only carry out this type of decision-making where the decision is either necessary for the entry into or performance of a contract, authorised by EU or UK law applicable to the data controller or it is based on the individual's explicit consent.