CILEX Community Privacy policy

This CILEX Community Website Privacy Policy is edited by CILEX (The Chartered Institute of Legal Executives), incorporated by Royal Charter and registered in England & Wales under number RC000850, whose principal office is at Kempston Manor, Kempston, Bedford, MK24 7AB (hereafter, the "**Data Controller**").

The Data Controller offers "The CILEX Community" Website (via a Hivebrite Account) (hereafter, the "**Platform**") to its users, which have subscribed on the Platform and as such have an User Account (hereafter, the "**Users**").

The CILEX Community Website is available at the following URL address: https://cilexcommunity.org.uk/

The Data Controller uses a solution called "Hivebrite", which enables the import and export of User lists and data, the management of content and events and the organisation of emailing campaigns.

In this regard, the Data Controller collects and processes the User's Personal Data, in accordance with the CILEX Community Website Privacy Policy and Cookies Policy.

The Data Controller commits to ensure that the compliance of the data processing is carried out by the Data Controller, in accordance with the UK Data Protection Legislation.

"UK Data Protection Legislation" means 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.

CILEX is not listed as a 'public body' for the purposes of the FOIA (Freedom of Information Act) and therefore, it is not under a duty to comply with the provisions of the FOIA.

The Data Controller has put in place an appropriate Privacy Policy, Cookies Policy and Terms of Service and Use for the CILEX Community Website to be fully transparent on how the Personal Data of Users are processed within the use of the Platform and Services provided.

CILEX have partnered with HiveBrite to bring you the CILEX Community. As such CILEX is deemed the Customer and so the data controller and HiveBrite the Company, so the Data Processor. All parties agree that the Customer shall be the Data Controller and the Company shall be deemed to be the Data Processor, with regard to the Users Data, as those terms are understood under the applicable Data Protection Laws. In such cases, the Parties agree to comply with the terms of the Data Processing Agreement (DPA), as available online at *https://hivebrite.com/legal/dpa* and as may be amended from time to time and CILEX's Data Sharing Agreement.

This Privacy Policy is intended for the Users of the Platform of the Data Controller and is in conjunction with the CILEX Privacy Notice, Privacy Statement and Code of Conduct, which are located on the CILEX Website.
The Data Controller has appointed a Data Protection Officer (hereinafter "DPO") that you may contact at the following address: privacyofficer@cilex.org.uk
Date of Last Update: 20/02/2024

ARTICLE 1. COLLECTED PERSONAL DATA

1.1 When Subscribing on the Platform

When subscribing to the Platform, the User is informed that its following Personal Data is collected for the purpose of creating an User Account:

Personal Data

- Personal Identification Data (First Name, Last Name, Gender, ID/Profile Photograph, Date of Birth, Language spoken, Nationality, Email Address, Phone Number and Address);
- Membership Number, Status and Grade
- Location Data
- Electronic Identification Data (IP Addresses, Cookies, etc.);
- Academic Curriculum and Results;
- Professional Experience/CV;
- Current Job;
- Professional Qualifications, University Education and Certificates;
- Hobbies and Areas of Interest;
- And more generally, any personal data submitted or posted by a User.

The User is informed that it is not possible to access the Platform without accepting the mandatory data strictly necessary to create an account and to authenticate the User.

Mandatory Data

- First Name;
- Last Name;
- Email Address;
- Membership Number, Status and Grade

1.2 During the Use of the Platform

The User may validly publish at its own initiative any content on the Platform, which shall be kept by the Company:

- Posts
- Events
- Profiles
- Networking Opportunities

The User is aware that when using the Platform, the User may decide to provide Sensitive Personal Data (also known as Special Categories of Personal Data) within the meaning set out in the UK Data Protection Legislation. By providing such Sensitive Personal Data, the User agrees to their data processing by the Platform in the conditions set forth in this Privacy Policy.

We may also collect Special Categories of Personal Data, such as gender, ethnicity, etc., whether you have a disability or any other protected characteristics (particularly related to where reasonable adjustments or access arrangements may be needed) and any information relating to a background check.

Such data will only be collected and/or provided to us, if you have provided your explicit consent or if we are otherwise permitted to receive and process it under the UK Data Protection Legislation.

For the processing of Special Categories of Personal Data, we consider whether the risks associated with our use of this type of Personal Data will affect our other obligations around data minimisation and security. A Data Protection Impact Assessment (DPIA) and an appropriate Policy document should be completed.

The lawful bases for Special Categories of Personal Data (also known as Sensitive Personal Data) can include one or more of the following lawful bases (and not all of which will be relevant to CILEX): Explicit Consent, Employment Law, Vital Interests, Charity or Not for Profit Bodies, Data manifestly made public by the Data Subject, Legal Claims, Reason for Substantial Public Interest,

Medical Diagnosis or Treatment, Public Health, Historical, Statistical or Scientific Purposes, processing for new purposes and processing not requiring identification.

Users 16 and Under

We do not knowingly collect or solicit Personal Data from anyone aged 16 or under or knowingly allow such persons to provide us with their Personal Data without Parental or Guardian consent. If you are aged 16 or under, please do not provide us with your Personal Data, without first asking your Parent or Guardian for their permission. In the event, that we learn that we have collected Personal Data from anybody aged 16 or under and we do not have the consent of a Parent or Guardian, we will delete that Personal Data, as quickly as possible. If you believe that we might have any Personal Data from or about anyone aged 16 or under without the consent of a Parent or Guardian, please send us a message by logging in to myCILEX Portal and go to Contact Us, then select 'Data Protection: Query and Request' on 'My Query Relates to' section. If you do not have access to the myCILEX Portal or do not wish to log your details on the system, please contact us by email at: privacyofficer@cilex.org.uk.

Storage of Data

Personal Data collected by CILEX is stored on secure IT systems. This Personal Data can generally be accessed throughout CILEX, except where it is unsuitable to do so, in which case appropriate measures are put in place to ensure Personal Data can only be accessed by those with a need to know.

No external person will have access to CILEX records, except in circumstances outlined in the CILEX Privacy Notice and Privacy Statement (available on the CILEX Website).

Any third-party contracted by CILEX to process Personal Data on its behalf will be requested to have security measures in place to protect the Personal Data and to treat such data, in accordance with UK Data Protection Legislation. We also set up Data Processing/Sharing Agreements with our third-party or supplier contracts. In the event of any contract relating to International Data Transfers, the additional applicable documents will be in place, such as EC SCCs (European Commission's Standard Contractual Clauses), IDTA (International Data Transfer Assessment) or ICO Addendum. CILEX has put in place procedures to deal with any Potential Data Security Incident (PDSI) and they will notify you and the UK's Information Commissioner's Office (ICO), when appropriate of any data breach, where we are legally required to do so.

ARTICLE 2. THE PURPOSE OF THE DATA PROCESSING

The Data Controller and its sub-contractors process Personal Data that are freely transferred by the User, when accessing the services proposed by the Platform for the following purposes:

Purpose	Lawful Basis/Bases
Creation and Management of a User Account.	Lawful Bases: Consent of the Data Subject, Contractual Necessity, Compliance with a Legal Obligation and Legitimate Interest.
Providing the User with all functionalities of the Platform, meaning: • *Sending invitations for events organised by the Data Controller or other Users, if the User has accepted to receive, such invitations;* • *Sharing content, including News, Resources and other Updates from the Data Controller or its Partners, if the User has accepted to receive, such offers.* • *Invite the User to events organised by the Platform.*	
Management of Data Subject's Rights of the Individual, according to the UK Data Protection Legislation and the Storage of User Personal Data;	
Making Statistics, in order: • *to improve the quality of the services proposed by the Platform;* • *To improve the usage functionalities of the Platform;*	
Making Statistics regarding the effective use of the Platform;	
Making Statistics regarding the different levels of activity on the Platform.	

ARTICLE 3. DATA RETENTION PERIOD

The Data Controller informs the User that the Personal Data related to the User Account is retained only, during the length of the User's subscription on the Platform.
Following the termination of the said subscription, the data collected upon the subscription, as well as the content published by the User on the Platform shall be deleted, after a period of 2 Years.

ARTICLE 4. INTERNATIONAL DATA TRANSFERS

The Users' data is stored in the European Economic Area (EEA) by the Data Controller, its subsidiaries and its trusted service providers. However, depending on the data processing, the Users' data may also be transferred to a country outside the EEA and to our trusted service providers and/or subsidiaries.
When transferring the data outside the EEA, the Data Controller ensures that the data is transferred in a secured manner and with respect to the UK Data Protection Legislation. When the country, where the data is transferred does not have a protection comparable to that of the EU, then the Data Controller uses "appropriate or suitable safeguards".
When the service providers to whom Personal Data is transferred are located in the United States, these transfers are governed by the Standard Contractual Clauses adopted by the EU Commission.
It is the responsibility of Hivebrite to have in place with its third-party providers the relevant documentation to ensure compliance with UK Data Protection Legislation and CILEX has a Data Processing Agreement in place with Hivebrite.
Hivebrite may transfer Personal Data to countries outside of the United Kingdom, where Personal Data is not protected in the same way (usually to other businesses, who provide services on their

behalf). In such cases, we will make sure that suitable safeguards are in place to protect the Personal Data, such as a signed Data Processing/Sharing Agreement, EC SCCs, IDTA and ICO Addendum, as applicable. Additional steps are taken to ensure that appropriate measures and controls are in place to protect that data, in accordance with the relevant UK Data Protection Legislation and Regulations.

Neither Party shall transfer Shared Data to any country outside the European Economic Area or the UK, unless that Party ensures that (as required to comply with applicable UK Data Protection Legislation):

• the transfer is to a country, territory or one or more specific sectors within a country approved by the UK's Information Commissioner's Office or the European Commission, as providing adequate protection and the prior written consent of the Data Subject/s.
• there are appropriate safeguards in place, as required by applicable UK Data Protection Legislation.
Or:
• it can rely on a derogation from the relevant obligations under the UK Data Protection Legislation.

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. This adequacy decision is due to be reviewed on 28th June 2025 with a view to this safeguard remaining in place for UK/EU Data Transfers.

ARTICLE 5. COMMITMENT OF THE DATA CONTROLLER

The Data Controller commits to process the User's Personal Data, in compliance the UK Data Protection Legislation and to undertake to, notably, to respect the following principles:

- Process the User's Personal Data lawfully, fairly and in a transparent manner;
- Only collect and process the Users' data for the strict purpose, as described under article 2 of the present Privacy Policy;
- Ensure that the Personal Data processed is adequate, relevant and limited to what is necessary, in relation to the purposes for which they are processed;
- Ensure that the Personal Data processed is accurate and if necessary is kept up-to-date and to take all reasonable steps to ensure that Personal Data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- Keep personal User's data for no longer than is necessary for the purposes for which they are processed;
- Put in place all necessary technical, organisational and security appropriate measures, in order to ensure the security, confidentiality, integrity, availability and the resilience of the process systems and services;
- Limit the access to the Users' data to the persons duly authorised to this effect;
- Guarantee to the Users their rights under the UK Data Protection Legislation, in relation to the processing of their Personal Data.

ARTICLE 6.EXERCISE OF THE USERS' RIGHTS OF THE INDIVIDUAL

The Rights of the Individual are:

- • The Right to be Informed – Data Subjects have the right to be informed about the collection, sharing, protection and use of their Personal Data.
- • The Right of Access – Data Subjects have the right to request access to any Personal Data that we hold concerning them.
- • 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 it is unable to be updated, this should be removed.
- • 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 (our right to get your data deleted | ICO).
- • The Right to Restrict Processing – Data Subjects have the right to request the restriction or suppression of their Personal Data, in certain circumstances.
- • 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 Right to Object – Data Subjects 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.
- • 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 and that is applicable to the Data Controller or it is based on the individual's explicit consent.

In certain cases, 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.

If you have any questions about how CILEX processes your Personal Data or you would like to exercise any of your Rights of the Individual under the UK Data Protection Legislation, log in to myCILEX Portal and go to Contact Us, then select 'Data Protection: Query and Request' on 'My Query Relates to' section. If you do not have access to the myCILEX Portal or do not wish to log your details on the system, please contact us by email at: privacyofficer@cilex.org.uk.

When processing is based on the User's consent, the right to withdraw consent at any time, without affecting the lawfulness of the processing based on consent, before its withdrawal.
In addition, in the event the User considers that its rights have not been respected, the User of which the Personal Data is collected can lodge a complaint, before the competent Data Protection Supervisory Authority. For any additional information, you can review your rights on the websites of the competent authorities.
The UK's Data Protection Supervisory Authority is:

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*

CILEX is registered, as a Data Controller at the UK Information Commissioner's Office under number Z7185599.

The competent EU Data Protection Supervisory Authorities are listed on the following website: Our Members | European Data Protection Board (europa.eu)

ARTICLE 7.USE OF COOKIES

The Data Controller informs the User that Hivebrite, as well as its sub-contractors, uses a tracking technology on its terminal, such as Cookies, whenever the User navigates on the Platform subject to the conditions described in the Data Controller's Cookies Policy on the CILEX Community Website.

ARTICLE 8.RECIPIENT AND PERSONS AUTHORISED TO ACCESS THE USERS' DATA

Only authorised persons working for the Data Controller and in some cases, its subsidiaries can access your Personal Data.

The Data Controller also uses trusted service providers to carry out a set of operations on their behalf for hosting. The Data Controller can also use service providers in the tech industry and editors of specific tools integrated into the Platform for technical purposes.

The Data Controller only provides service providers with the information that they need to perform the service and ask them not to use your Personal Data for any other purpose. All of these trusted service providers should only process the Personal Data on our documented instructions and provide sufficient guarantees, in terms of confidentiality, expert knowledge, reliability and resources, to implement technical, organisational and security measures, which will meet the requirements of the applicable legislation, including for the security of processing.

The Data Controller may be required to disclose or share your Personal Data to comply with a legal obligation or to enforce or apply our terms of use/sale or any other conditions that you have accepted; or to protect the rights, safety or property of CILEX, its customers or employees.

List of the Main Hivebrite Service Providers:

Service Provider	**Service**	**You can consult the privacy policy by clicking on the following link:**
KIT UNITED 44 rue la fayette 75009 Paris France	HIVEBRITE solution	https://hivebrite.com/privacy-policy

Stripe 510 Townsend Street San Francisco CA 94103, USA	Payment Service	https://stripe.com/fr/privacy
PayPal 21 rue Banque 75002 Paris France	Payment Service	https://www.paypal.com/us/webapps/mpp/ua/privacy-full
Google Cloud Platform Gordon House, 4 Barrow St, Dublin, Ireland	Hosting of all data and content produced/provided by the User, as well as images, profile pictures and back-ups.	https://cloud.google.com/security/privacy/
Amazon AWS 38 avenue John F. Kennedy, L-1855, Luxembourg		https://aws.amazon.com/compliance/gdpr-center/
Sentry 132 Hawthorne Street, San Francisco, CA 94107 USA	Production and Storage of Error Logs enabling our Developers to correct the code.	https://sentry.io/privacy/
SendGrid 375 Beale Street, Suite 300, San Francisco, CA 94105 USA	Sending of Emails from the Platform.	https://api.sendgrid.com/privacy.html
Hivebrite, Inc. 16 Nassau St, New York, NY 10038, USA	Customer Support for the Platform.	https://hivebrite.com/privacy-policy

For the full up-to-date list of Hivebrite Sub-Processors, please view this link:
Hivebrite | Sub-processors