EUROCALL Data Protection Policy

This statement outlines how the EU General Data Protection Regulation (EU GDPR), the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 relates to EUROCALL. Under the Data Protection legislation, EUROCALL has an obligation to protect all the data it holds legitimately.

As we are a member organisation, it is legitimate that we hold information for the purposes of contact regarding our research and educational activities. All the personal information given to us by members is processed in accordance with the Data Protection legislation. This Data Protection Policy sets out how EUROCALL processes personal data entrusted to it by its members.

The EUROCALL Executive Committee is the Data Controller for the Association. The Data Control Leads are the Honorary Secretary and Treasurer of the Association.

Control of Data

Data Protection Principles
All processing of Personal Data comply with the seven Data Protection principles contained within the UK GDPR. In summary, the Data Protection principles require that Personal Data is:

(i) processed lawfully, fairly and in a transparent manner (**Lawfulness, Fairness and Transparency**);
(ii) (ii) collected only for specified, explicit and legitimate purposes and not processed in a manner incompatible with those purposes **(Purpose Limitation**);
(iii) adequate, relevant and limited to what is necessary in relation to the purpose(s) for which it is processed (**Data Minimisation**);
(iv) accurate and kept up to date (**Accuracy**);
(v) not kept in a form which permits identification of individuals for longer than is necessary for the purpose(s) it is processed (**Storage Limitation**);
(vi) Processed in a way ensures its security and to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage (**Integrity and Confidentiality**); and
(vii) responsible for demonstrating compliance with the above listed principles (**Accountability**).

These seven Data Protection principles are the foundation on which the remainder of the legislation is built and so all EUROCALL members must be mindful to comply with these principles at all times.

Lawful Basis for Processing Personal Data
In compliance with the first Data Protection principle set out above, Personal Data must be processed fairly, lawfully and in a transparent manner for specified purposes. UK GDPR requires that processing of Personal Data must be for one or more lawful purposes under Article 6 of UK GDPR, known as a “lawful basis”.

Information on the categories of data and our lawful basis for processing your data can be found in our Privacy Notice.

Purpose Limitation
Personal information will only be used for the normal business of the Association and no other, without further consent. This information will be used for the following purposes:
- To enable you to register for EUROCALL events, including the EUROCALL conference
- To enable EUROCALL to contact you, by email, on EUROCALL-related matters
- To enable you to apply for or to renew your membership of EUROCALL
- To enable us to fulfil our obligations to you as a EUROCALL member
- To enable you to take part in EUROCALL activities

EUROCALL uses abstract management and peer-review systems supported by external agencies for the processing of conference paper submissions. These services are anonymised and password protected, and the personal information is kept no longer than the end of the calendar year in which the conference occurs. Conferences often make use of a conference app: this will be determined by the conference organisers. These external sites have their own privacy policies.

Third Party Information
EUROCALL may only share the Personal Data entrusted to it with third parties, such as its service providers or other public bodies, if:

- they have a need to know the information for the purposes of providing the contracted services;
- sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;
- the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- the transfer complies with any applicable cross-border transfer restrictions; and
- a data sharing agreement has been entered.

- The only third party with whom third party member information is shared is Cambridge University Press. They hold the names and contact details for members who receive copies of the journal, ReCALL, and of authors and reviewers on a secure server.
- No information will be shared with any other body unless at the behest of the member concerned.
- In all cases, only the minimum necessary amount of data will be retained.
- The information EUROCALL holds will be accurate.
- The information will be kept up-to-date and outdated information deleted.
- Members' data will only be retained while an individual remains a fully-paid-up member of the Association. Information on former members will only be retained until end of the calendar year in which their membership lapses. After that period, information on former members shall not be retained.

Members' Information Rights

Under the Data Protection legislation, a Data Subject has the following rights, all of which are qualified in different ways:

(i) The right to be informed: a Data Subject has the right to be informed about the collection of their Personal Data and to be informed of how their Personal Data is being used by EUROCALL. This is a key transparency requirement under the UK GDPR.

(ii) The right of access to your Personal Data: a Data Subject has the right to request access to their Personal Data held by EUROCALL, which is known as a "Subject Access Request".

(iii) The right to rectification: a Data Subject has the right to have inaccurate Personal Data held by EUROCALL rectified or completed if it is incomplete.

(iv) The right to be forgotten: a Data Subject has the right to have their Personal Data held by EUROCALL erased. This right is not absolute and only applies in certain circumstances as detailed in Article 17 of UK GDPR.

(v) The right to restrict processing: a Data Subject has the right to restrict processing of their Personal Data. This right is not absolute and only applies in certain circumstances as detailed in Article 18 of UK GDPR.

(vi) The right to data portability: a Data Subject has the right to receive copies of their Personal Data in a machine readable and commonly used format. This right is not absolute and only applies in certain circumstances as detailed in Article 20 of UK GDPR.

(vii) The right to object: a Data Subject has a right to object to the processing of their Personal Data. This right is not absolute and only applies in certain circumstances as detailed in Article 21 of UK GDPR.

(viii) Rights in relation to automated decision making and profiling: a Data Subject has a right not to be subject to a decision based solely on automated decision-making using their Personal Data without any human involvement. Profiling (Automated Processing of Personal Data to evaluate certain things about an individual) can be part of an Automated Decision-Making process. This right is not absolute and only applies in certain circumstances as detailed in Article 22 of UK GDPR.

To exercise your Data Protection Rights, please contact eurocall@ulster.ac.uk. EUROCALL undertakes to consider and act upon a request without undue delay. In compliance with the Data Protection legislation, this will be at the latest within one month of receipt of a request. However, that period may be extended by 2 further months where necessary, taking into account the complexity and number of the requests.

Breach notification

In the event of a data breach, EUROCALL will notify you without undue delay after we have been made aware of the data breach and ascertained what personal data have been affected.

EUROCALL shall investigate all incidents of a suspected or actual Personal Data Breach and take appropriate action to mitigate the consequences and prevent similar events occurring in the future. Should the investigation confirm that a Personal Data Breach has in fact occurred, EUROCALL shall notify the ICO, where required, notify the Data Subject and update the Data Breach Register accordingly.

The EUROCALL Executive is continually identifying and addressing emerging privacy and security risks and updating this policy statement accordingly.

International Transfers

There are restrictions imposed on EUROCALL by Data Protection legislation when transferring Personal Data outside the UK or the EU/EEA (a "restricted transfer") to ensure the same level of protection is afforded to individuals' Personal Data. EUROCALL is permitted to make restricted transfers so long as they comply with certain conditions, namely:

(i) where the UK have approved the recipient country as having adequate data protection laws and procedures (known as an "adequacy regulation"); or

(ii) where the EUROCALL have put in place certain safeguards in accordance with the Data Protection Legislation, which will typically take the form of entering an approved form data sharing agreement called the International Data Transfer Agreement; or

(iii) there is an exemption available so that EUROCALL can proceed with the Restricted Transfer in absence of (i) or (ii) above.

Most frequently, EUROCALL will proceed to make a restricted transfers in reliance of adequacy regulations.

Complaints

An individual has the right to make a complaint if they feel that their personal information has not been handled by EUROCALL in accordance with the Data Protection legislation. A complaint may be submitted in writing to eurocall@ulster.ac.uk. Alternatively, a complaint may be made to the Office of the Information Commissioner.