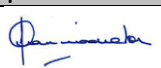


# CIGRE UK Information Security Management Policy on Personal Data

Revision	Date	Description	By	Reviewed	Approved
0	22/07/2021	First Issue	Martin Ansell	John Finn	

# CIGRE UK Information Security Management Policy on Personal Data

## 1. Purpose

In the course of its business, it is necessary for CIGRE UK to collect, process, transmit, store and otherwise handle personal data of members. This policy provides the basis for protecting such data while ensuring compliance with the legal requirements of the Data Protection Act 2018 (DPA2018) and the UK General Data Protection Regulation (UK GDPR)

This data will be used for communication purposes for CIGRE only

## 2. Scope

This policy relates to all personal data collected, processed, transmitted, or stored (the term processed will be used throughout the remainder of this document) by CIGRE UK. All CIGRE UK members shall adhere to this Policy.

## 3. Policy

It is CIGRE UK's responsibility to ensure that an individual's right to privacy is safeguarded, personal data is used only as intended and that precautions preventing misuse are both effective and appropriate. Personal data will therefore be:

3.1 Processed lawfully, fairly and in a transparent manner in relation to individuals

3.2 Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes

3.3 Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

3.4 Accurate and, where necessary, kept up to date; every reasonable step will be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased or rectified without delay;

3.5 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical

purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

3.6 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, using appropriate technical or organisational measures.

3.7 Modified when the Secretary or nominated person is notified of changes.

3.8 Centrally stored and managed under the ownership of the Secretary or nominated persons.

#### **4. Risks**

Breach of legal requirements concerning personal data, may result in reprimand, censure, enforcement proceedings, fines, and/or damages. It may also result in personal liability for any CIGRE UK delegated members and/or officers processing the data on behalf of the controller, adverse publicity and damage to CIGRE UK's reputation.

#### **5. Implementation**

The CIGRE UK Secretary shall assign responsibility to any delegated member using the data to manage data privacy issues and report on compliance with this Policy.

Specific guidance is given in Appendices A-E with regard to the membership application process and storage of membership records, marketing, event registration, surveys and technical activities.


For communications with multiple recipients who are not covered by one of the examples covered by these Appendices, then emails should be addressed to the sender with all of the intended recipients entered in the back copy (bcc) field so that their email addresses are not made available to a wide audience.

#### **6. Policy Awareness**

A copy of this policy statement will be made available on the CIGRE UK web-site accessible to all members and interested parties.

#### **7. Review**

Policy reviews are to be undertaken annually as part of an annual executive meeting.



## Appendix A Membership Application Process and storage of Membership Records.

### A1 Membership Applications

#### A1.1 Applications made using Jotform

Membership applications are completed on a purpose designed Jotform gathering the specific data required for CIGRE membership. It should be noted that no financial details of the member are ever taken. On completion and submission of the form it is automatically recorded in a spreadsheet within Jotform. The data from one application form appears as one row in the spreadsheet. The spreadsheet is downloaded approximately twice per week in Excel format to enable processing of the applications. Each time an updated spreadsheet is stored in Drop Box and the old spreadsheet is deleted.

- a) For individual Members IM1 or Collective Members, the Secretary will transfer the data from the Jotform spreadsheet into the current password protected Master Membership spreadsheet (also held in Drop Box). An invoice will then be generated and sent to the Individual member or Representative of the Collective Membership. Upon receipt of the payment the Secretary will activate the membership in the CIGRE Central Office National Committee Database (NCDB).
- b) For Individual Members IM2 or those who have asked for NGN membership, the Secretary will advise the NGN membership team that one or more new NGN applications have been received and list the names. The NGN membership team will then access the Jotform spreadsheet and process it transferring the details to the password protected NGN master membership spreadsheet. After checking eligibility, if the new person is to receive a subsidised membership then the NGN membership team will advise the Secretary the name of the subsidised member and the Secretary will enter the details into the NCDB and activate the membership and also ensure the member details are on the master membership spreadsheet.
- c) For Student members, the Secretary will advise the NGN membership team that one or more Student applications have been received and list the names. The NGN membership team will process the application including entering the details into the NCDB and activating the Student membership. They will also keep the details in a password protected Master Student membership spreadsheet in Drop Box accessible by the Secretary and the NGN membership team.

#### A1.2 Applications received from Central Office.

Although the majority of applications for membership of CIGRE UK are received via Jotform a small number of people apply to Central Office. Central office gather these applications, approximately monthly, in an excel file which is sent by email to the CIGRE UK Secretary. On receipt of the email the Secretary will add the new rows to a consolidated file of Central office applications stored in dropbox and delete the Central office excel file. This folder can be accessed by the Secretary and the NGN membership team.



From this point on the application will be processed in the same way as a) to c) above. For NGN/IM2 memberships and Student memberships the Secretary will advise the NGN membership team to check the Central Office spreadsheet and process accordingly.

## **A2 Membership Records**

The records of all CIGRE UK members are held in one of the following password protected files in Drop Box

- a) The Master membership spreadsheet in Drop Box
- b) The NGN Master membership spreadsheet in Drop Box
- c) The NGN Master Student membership spreadsheet in Drop Box

Members should normally advise the Secretary of any changes in

- Employing Company
- Position in Company
- Email address
- Contact telephone number
- Postal address

On notification of a change the Secretary will update the record if in a) or advise the NGN membership team if the information is held in b) or c).

The data in these records is used mainly for the issuance of annual renewal invoices or contact with the member with regard to their membership status or any other CIGRE related business.

## **A3 Summary of Process**

The flow of the process, together with the storage locations, data held, access permissions and security are shown in the Table on the next page.

Membership Data Management - Folders and Files						
Platform	Account	Applications	Folder/File	Data Held	Access Permissions	Security
Jotform	CIGRE UK	Online Form		Personal (name, email address, Company, role, gender, DofB, tel. no., CIGRE interests	Administrator: MA	User Name and password
↓						
Dropbox	CIGRE UK	Secure Cloud storage	Membership application spreadsheet	As for Jotform	Administrator: MA UKNC Secretary:JF NGN Membership team:HY	Password protected file
			Master Membership spreadsheet	Personal (name, email address, Company, role, gender, DofB, tel. no.	Administrator: MA UKNC Secretary:JF Financial Controller:AR Membership WG Lead:DJ	Password protected file
			NGN Master Membership spreadsheet	Personal (name, email address, Company, role, gender, DofB, tel. no.	Administrator: MA UKNC Secretary:JF NGN Membership team:HY	Password protected file
			Student Master Membership spreadsheet	Personal (name, email address, Company, role, gender, DofB, tel. no.	Administrator: MA UKNC Secretary:JF NGN Membership team:HY	Password protected file
↓						
NCDB	CIGRE CO		CIGRE CO Membership Management Database	Personal (name, email address, Company, role, gender, DofB, tel. no.	Administrator: CIGRE CO UKNC Secretary:JF NGN Membership team: HY for Students only	User Name and password



## Appendix B Marketing Data

Marketing Information is held securely on a MailChimp account. The data is limited to name, email address and company/organisation (optional). Access is limited to named individuals.

When signing up the recipient gives permission to receive marketing emails from CIGRE UK. Each marketing e-shot includes an option to update your details and unsubscribe if you do not wish to receive further emails. The database is for CIGRE UK purposes only and is not shared with third parties.



## Appendix C Event Registration Data

Information is held securely on an Eventbrite account. The data is limited to name, email address and company/organisation and job function. Access is limited to named individuals.

The registrant may also be asked to confirm CIGRE membership, and confirm that they have read and understood CIGRE's meeting compliance regulations. In the case of events with catering, they will be asked about their dietary requirements. The database is for CIGRE UK purposes only and not shared with third parties





## Appendix D Survey Monkey

From time-to-time CIGRE may ask its members to engage in a survey in which it may be offered as an option to provide their name, email address and company/organisation. This information is held securely on a SurveyMonkey account.



## Appendix E Technical Activities

Within CIGRE UK we have a Technical Committee which includes the Chair and the sixteen Regular Members for the Study Committees. It is clearly important for them to be involved in communications within the technical community. However, to protect their privacy rights, if any of their personal data (particularly email address) is to be shared openly within the technical community, they should have explicitly agreed that they are happy for this to happen. To enable this agreement and to have it recorded a special JotForm is available which can be accessed by clicking on the following link

<https://form.jotform.com/210622428423346>

Anyone participating in the above-mentioned technical activities should click the link and complete their acceptance.