BRITISH COUNCIL

BRITISH COUNCIL
DATA PROTECTION CODE FOR PARTNERS AND SUPPLIERS

CONTENTS

PURPOSE OF THE CODE

The British Council takes data protection seriously. This code sets out our commitment to protecting personal data when working with partners and suppliers. It does not constitute a contract between the British Council and its partners.

SCOPE OF THE CODE

This code applies where personal data is exchanged between the British Council and:

- Suppliers of goods and services.
- Project partners.

It covers data sharing arrangements where the British Council and its partners exercise joint control over the data, as well as data processing arrangements in which one side processes data on the instructions of the other.

Personal data means any information relating to an identifiable living person, i.e. the information is obviously about that person or is capable of being used to learn, record or decide something about them. It does not have to be confidential or private and could relate to anyone, including employees, students, project participants and members of target audiences.

THE BRITISH COUNCIL'S DATA PROTECTION COMMITMENT AND EXPECTATIONS

The British Council's global policy is to work to the data protection principles in the UK Data Protection Act 2018, unless more stringent local law applies. These principles represent the minimum international standard the British Council operates to in the absence of more stringent local regulation.

The British Council expects its delivery partners and suppliers to work to the same minimum standards. This means that in any data sharing or data processing arrangement with the British Council, the personal data will:

- Be obtained and used in ways that are fair to the individual – the British Council and its partners or suppliers will be transparent over what they do with the data and who they disclose it to; will only use it in ways the individual might reasonably expect and do nothing that would have an unjustifiably adverse effect on the individual.
- Be obtained and used only for specified and legitimate purposes – the British Council and its partners or suppliers will be clear about their reasons for using the data and do nothing incompatible with those purposes.
- Be maintained to appropriate quality and retention standards – the British Council and its partners or suppliers will ensure the data is relevant, adequate and accurate for its purpose and retained for no longer than is necessary.
- Be handled in line with the individual's rights, primarily to access their data – the British Council and its partners or suppliers will aim to disclose personal data on request provided it does not compromise the privacy of others.
- Be protected from unauthorised use and disclosure or against accidental loss, destruction and damage – the British Council and its partners or suppliers will take appropriate measures to guard personal data against such risks, and where appropriate provide evidence of compliance with ISO/IEC 27001.
- Not be transferred to other countries unless there is adequate protection for the rights of individuals in relation to their personal data – the British Council and its partners or suppliers will ensure adequate protection exists before making such transfers.

The British Council recognises that it will be necessary to depart from or limit these principles in situations corresponding to the exemptions in the UK Data Protection Act 2018. For example, in order to comply with local law or official functions; to meet existing obligations on disclosure and confidentiality; to facilitate legal proceedings and negotiations; to prevent crime and to enable special purposes such as research and journalism.

DATA SHARING

Where the British Council and a partner have a data sharing arrangement, i.e. they both exercise control over a set of personal data, they will (unless agreed otherwise):

- Only collect and use the personal data for the purposes that have been agreed or are clearly implied by the circumstances.
- Not transfer or disclose the personal data to third parties without the consent of the other unless it has already been agreed or is clearly implied by the circumstances.
- Not transfer the personal data to other countries without first notifying the other unless the transfer has already been agreed or is clearly implied by the circumstances.
- Use, where appropriate, EU Standard Contractual clauses to protect personal data being transferred outside the European Economic Area.
- Promptly notify each other of any data breaches, complaints or access requests in respect of the personal data and assist in resolving them.
- Co-operate in meeting the standards contained in this code including, where appropriate, being audited on compliance procedures.

DATA PROCESSING

In addition to the data sharing commitments, where the British Council and a supplier have a data processing arrangement, i.e. the supplier processes the data on behalf, or on the instructions, of the British Council, they will:

- Ensure the processing is carried out under a written contract in which the supplier processes the data on the instructions of the British Council.
- Ensure the contract requires the processor takes appropriate measures to protect the data from unauthorised or unlawful processing and from accidental loss, damage or destruction.

ACTING ON THE CODE

Adherence to this code should be proportionate to the circumstances. The level of protection will depend on the expectations of the data subjects, the sensitivity of the data and the likely consequences of its loss or misuse.

The British Council use this code during procurement to make its commitment to data protection clear and to seek suppliers and partners who demonstrate a similar commitment. Example questions the British Council may ask at procurement are included in the appendix.

This code is for guidance only and does not constitute a contract.

APPENDIX 1: EXAMPLE QUESTIONS AND REQUIREMENTS FOR PROSPECTIVE SUPPLIERS

These examples are for illustration only and are not necessarily the ones that will be used in an actual supply situation.

Pre-qualification questionnaire:

1. Is the supplier registered with [insert name of national data protection regulator]? If so, please give the name in which the supplier is registered.
2. Has the supplier or any of its subcontractors been subject to an investigation or any finding, decision, notice or undertaking by any court or [insert name of national data protection regulator]? If so, please give details.
3. Will the supplier use subcontractors? If so, please identify all subcontractors, their functions and geographic locations.
4. Will the supplier or any subcontractors be transferring the data outside [insert name of country]? If so, please give details.

Invitation to tender:

1. What organisational and technical measures does the supplier (and subcontractor) have in place to guard against the unlawful or unauthorised processing of the data and to protect it from accidental loss, damage or destruction?

   In practice this might be broken down into further questions depending on the scenario, for example access control, encryption of data, secure transmissions, data deletion, staff access and training.
2. Please confirm where the data, including any backups, will be hosted.
3. Is the supplier (and subcontractor) certified against ISO/IEC 27001? If so, please provide a copy of certification.
4. Is the supplier (and subcontractor) a member of [insert name of voluntary data protection scheme, e.g. US Privacy Shield]?

APPENDIX 2:
USEFUL SOURCES

UK Information Commissioner
www.ico.org.uk

ISO/IEC 27001 (information security standard)
http://en.wikipedia.org/wiki/ISO/IEC_27001