global mediation

Data protection policy

CMC CIVIL MEDIATION COUNCIL

College of Mediators Approved Mediator

The Organisation needs to collect and use certain types of information about staff, clients and other individuals who come into contact with the company in order to operate. In addition, it may be required by law to collect and use certain types of information to comply with statutory obligations of Local Authorities, government agencies and other bodies.

This personal information must be dealt with properly, however it is collected, recorded and used — whether on paper, in a computer, or recorded on other material — and there are safeguards to ensure this is within the UK General Data Protection Regulation and the Data Protection Act 2018.

We regard the lawful and correct treatment of personal information as very important to successful operations, and to maintaining confidence between those with whom we deal and ourselves. We ensure that our Organisation treats personal information lawfully and correctly.

Most businesses hold personal data on their customers, employees and partners. The explosion in the use of the Internet, electronic communication and computerisation of business data has led to an increase in the importance of privacy. Breaches of computerised data security have prompted the introduction of legislation.

These include:

1. Human Rights Act 1998
2. Freedom of Information Act 2000
3. Privacy and Electronic Communications Regulations 2003
4. Regulation of Investigatory Powers Act 2000
5. Telecommunications (Lawful Business Practice) Interception of Communications Regulations 2000
6. Data Protection Act 2018
7. Computer Misuse Act 1990
8. UK General Data Protection Regulation (UK GDPR).

Following Brexit the UK adopted the UK General Data Protection Regulations and amended the Data Protection Act 2018 replacing the EU General Data Protection Rehulations within the UK. Its purpose is to protect the "rights and freedoms" of living individuals, and to ensure that personal data is not processed without their knowledge, and, wherever possible, that it is processed with their consent.

The top management of Global Mediation Limited are strongly committed to the rights of individuals whose data they collect and process and will comply with UK GDPR and Data Prtoection Act 2018 related to personal information in line with the UK General Data Protection Regulation (UK GDPR).

The top management of Global Mediation Limited ensures that it meet its requirements under UK GDPR for the management of personal information, that the objectives of Global Mediation Limited and obligations under the law are met, and ensures that controls are in place that reflect the level of risk that Global Mediation Limited is willing to accept. In addition, steps are taken to ensure that Global Mediation Limited is able to meet all the regulatory, statutory and contractual obligations that are applicable, including the protection of the interests of individuals and all other relevant stakeholders.

To comply with the requirements of GDPR, Global Mediation Limited will:

1. Process personal information only where this is strictly necessary for legitimate organisational purposes
2. Collect only the minimum personal information required for these purposes and not process excessive amounts of personal information
3. Provide clear information to individuals about how their personal information will be used and who will be using the information
4. Only process relevant and adequate personal information
5. Process personal information fairly and lawfully
6. Keep all personal information secure
7. Maintain an inventory of the categories of personal information that is processed
8. Ensure they keep personal information accurate and up to date
9. Retain personal information only for as long as is necessary for legal or regulatory reasons or, for legitimate organisational purposes
10. Respect individuals' rights in relation to their personal information as defined in the UK GDPR
11. Only transfer personal information outside the EU Member States in circumstances where it can be adequately protected and aligned with UK GDPR Regulations
12. Only apply exemptions permitted by data protection legislation
13. Identify internal and external stakeholders and the degree to which these stakeholders are involved in the governance of Global Mediation Limited's stored or processed personal information
14. Identify staff with specific responsibility and accountability for the ongoing maintenance and support of the requirements of the GDPR.
15. Notification to the Information Commissioner's Office (ICO)
16. Global Mediation Limited has notified the Information Commissioner that it is a data controller and/or processor and that it processes personal data. Global Mediation Limited has identified and recorded all the personal data that it processes in the Data Register.
17. A record of notification to the ICO is retained by the DPO and the ICO Notification Handbook is used as the authoritative guidance for notification. This notification is reviewed annually and update notifications are issued accordingly.

18. The DPO is responsible for reviewing the details of notification to ensure that any changes to the way that Global Mediation Limited processes or controls personal data is (as determined by changes to the Data Register and following management review) referred back to the ICO. Additional requirements for notification may also arise from Personal Data Impact Assessments.
19. The policy applies to all Employees and Processors of Global Mediation Limited such as outsourced suppliers. Any breach of the GDPR will be considered as a breach of the disciplinary policy and could also be considered a criminal offence, potentially resulting in prosecution.

All third parties working with or for Global Mediation Limited, and who have or may have access to personal information, will be expected to comply with this policy. All third parties who require access to personal data will be required to sign a confidentiality agreement before access is permitted. This agreement will ensure that the third party has the same legal obligations as Global Mediation Limited. This will also include an agreement that Global Mediation Limited can audit compliance with the agreement.

GDPR will apply to all controllers that are established in the UK (United Kingdom) who process the personal data of data subjects, in the context of that establishment.

Key definitions

Personal data: this is defined as 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 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 (i.e. sensitive data) personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or 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 the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

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: 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 profiling and a right to be informed about the existence of profiling, of measures based on 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 controller to report personal data breaches to the supervisory authority (usually the Information Commissioner's Office) where the breach is likely to adversely affect the personal data or privacy of the data subject.

Data subject consent: 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. The processing of personal data of a child under 13 years of age is only lawful if parental or custodian consent has been obtained.

Third party: anatural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, is authorised to process personal data.

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

Company responsibilities

Global Mediation Limited is a data processor as defined under the GDPR.

Senior Management and all those in managerial or supervisory roles throughout Global Mediation Limited are responsible for developing and encouraging good information handling practices within the organisation; responsibilities are set out in individual job descriptions.

A Data Protection Officer, a member of the senior management team, is accountable to the top management of Global Mediation Limited for the management of personal information within Global Mediation Limited and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes the development and implementation of security and risk management to ensure compliance.

Global Mediation Limited has appointed a suitably qualified and experienced Data Protection Officer (DPO) who is responsible for day-to-day compliance with this policy. The DPO is responsible for ensuring that Global Mediation Limited complies with the GDPR in relation to all aspects of data processing. The DPO has direct responsibility for policy and procedures, including Subject Access Requests. The DPO is also the person to whom all staff will go to seek guidance regarding GDPR compliance.

It should be noted that compliance with GDPR requirements remains the responsibility of all staff who process or control personal information for Global Mediation Limited. All members of staff employed by Global Mediation Limited are also responsible for ensuring that any personal data that is about them that is supplied by them to Global Mediation Limited is accurate and up to date.

The Training Policy defines specifically what training is required for all staff, including specific roles.

Risk assessment in relation to GDPR

Global Mediation Limited needs to ensure that it is aware of any risks associated with the processing of all types of personal information. A Data Impact Assessment procedure has been implemented and is used by Global Mediation Limited to assess any risk to individuals during processing of their personal information. Data Impact Assessments will also be completed by Global Mediation Limited for any processing that is undertaken on their behalf by any third party organisation prior to their onboarding. Global Mediation Limited will also, through the application of the Data Impact Assessment procedure, ensure that any identified risks are managed appropriately to reduce the risk of non-compliance. The DPO will oversee these assessments to confirm the third party's compliance with GDPR and organisational policies.

Where processing of personal information may result in a high risk to the "rights and freedoms" of natural persons, Global Mediation Limited shall complete a data protection impact assessment, prior to conducting the processing, to ensure the personal information is protected. This assessment may also be used to apply to a number of similar processing scenarios with a similar level of risk.

Where, as a result of a Data Protection Impact Assessment, it is clear that Global Mediation Limited will process personal information in a manner that may cause damage and/or distress to the data subjects, the DPO must review the process before Global Mediation Limited proceeds to process the information. If the DPO decides that there are significant risks to the data subject they will escalate to the ICO for final guidance.

The Organisation shall apply selected controls for the ISO 27001 Annex A to reduce risk. This should also reference Global Mediation Limited's risk acceptance criteria and the requirements of the GDPR.

Principles of data protection

Any processing of personal data must be conducted in accordance with the following data protection principles of the Regulation, and Global Mediation Limited's policies and procedures will ensure compliance.

Personal data must be processed lawfully, fairly and transparently. Global Mediation Limited's Fair Processing Procedure details how this is achieved.

The GDPR introduces the requirement for transparency whereby the controller has transparent and easily accessible policies relating to the processing of personal data and the exercise of individuals' 'rights and freedoms'.

Information must be communicated to the data subject in an intelligible form using clear and plain language.

The specific information that must be provided to the data subject must as a minimum include:

1. The identity and the contact details of the controller and, if any, of the controller's representative
2. The contact details of the Data Protection Officer, where applicable
3. The purposes of the processing for which the personal data are intended as well as the legal basis for the processing
4. The period for which the personal data will be stored
5. The existence of the rights to request access, rectification, erasure or to object to the processing
6. The categories of personal data concerned
7. The recipients or categories of recipients of the personal data, where applicable

8. Where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data
9. Any further information necessary to guarantee fair processing.

Personal data can only be collected for specified, explicit and legitimate purposes. Data obtained for specified purposes must not be used for a purpose that differs from those formally notified to the Information Commissioner as part of Global Mediation Limited's GDPR registration.

Personal data must be adequate, relevant and limited to what is necessary for processing. The Data Protection Officer is responsible for ensuring that information, which is not strictly necessary for the purpose for which it is obtained, is not collected.

All data collection methods (electronic or paper-based), including data collection requirements in new information systems, must be approved by the Data Protection Officer and approval recorded.

The Data Protection Officer will ensure that all data collection methods are reviewed annually by internal audit or external experts to ensure that collection continues to be adequate, relevant and not excessive.

The DPO is responsible for ensuring that any data that is shown to have been obtained excessively, or is not specifically required by Global Mediation Limited, is securely deleted or destroyed (see A.8.3.2 and A.11.2.7).

Other considerations

Personal data must be accurate and kept up to date.

Data that is kept for a long time must be reviewed and updated as necessary. Any data that is considered to be inaccurate or likely to be inaccurate must be removed.

Top management is responsible for ensuring that all staff are trained in the importance of collecting accurate data and maintaining it.

All individuals are responsible for ensuring that any data held by Global Mediation Limited is accurate and up to date. Any data submitted by an individual to a company, such as via a registration form, will be considered to be accurate at the time of receipt.

Employees or other individuals should notify Global Mediation Limited of any changes in personal information to ensure personal information is kept up to date. It is the responsibility of Global Mediation Limited to ensure that any notification of changes to personal information is implemented.

The DPO is responsible for ensuring that all necessary actions are taken to ensure personal information is accurate and up to date. This should also take into account the volume of data collected, the speed with which it might change and any other relevant factors.

The DPO will review, at least once a year, all the personal data processed by Global Mediation Limited, held in the Data Register. The DPO will note any data that is no longer required in the context of the registered purpose and will ensure that it is appropriately removed and securely disposed of (see A.8.3.2 and A.11.2.7).

If a third party organisation has provided inaccurate or out-of-date personal information, the DPO is responsible for informing them that the personal information is inaccurate and/ or out-of-date and will advise them that the information should no longer be used. The DPO should also ensure that any correction to the personal information is passed on to the third party.

Personal data considerations

Personal data must be kept in a form such that the data subject can be identified only as long as is necessary for processing.

Where personal data is retained beyond the processing date, it will be encrypted in order to protect the identity of the data subject in the event of a data breach.

Personal data will be retained in line with the retention of records procedure and, once its retention date is passed, it must be securely destroyed as set out in the Retention of Records Procedure.

The DPO must specifically approve any data retention that exceeds the retention periods defined in the Retention of Records procedure and must ensure that the justification is clearly identified and in line with the requirements of the data protection legislation.

This approval must be written.

Personal data must be processed in a manner that ensures its security.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. These controls have been selected on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed. Security controls will be subject to audit and review.

Global Mediation Limited's compliance with this principle is contained in its Information Security Management System (ISMS), which has been developed in line with ISO/IEC 27001: 2013 and the Security Policy set out in the ISMS.

Personal data shall not be transferred to a country or territory outside the United Kingdom unless that country or territory ensures an adequate level of protection for the 'rights and freedoms' of data subjects in relation to the processing of personal data.

Transferring personal data to a country outside the UK

The Company may, from time to time, transfer ('transfer' includes making available remotely) personal data to countries outside of the UK. The UK GDPR restricts such transfers in order to ensure that the level of protection given to data subjects is not compromised.

Personal data may only be transferred to a country outside the UK if one of the of following applies:

a. The UK has issued adequacy regulations confirming that the personal data will receive an adequate level of protection (referred to as 'adequacy decisions', 'adequacy regulations', or 'partial findings of adequacy'). Such regulations may apply to a country as a whole, organisation(s), framework(s) or mechanism(s), or to data covered by specific legislation. Since 1 January 2021, transfers of personal data from the UK to EEA countries have continued to be permitted. Pre-existing EU Commission adequacy decisions in effect as at 31 December 2020 are also recognised, subject to ongoing review by the UK Government.

b. Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct, or an approved certification mechanism. Standard contractual clauses include the International Data Transfer Agreement issued by the Information Commissioner's Office and the International Data Transfer Addendum to the current EU Commission Standard Contractual Clauses (set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021), issued by the Information Commissioner's Office. (Contracts entered into on the basis of the old EU Commission Standard Contractual Clauses prior to 21 September 2022 will continue to provide appropriate safeguards until 21 March 2024.)

c. The transfer is made with the informed and explicit consent of the relevant data subject(s).

d. The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the data subject and the Company; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for the Company's legitimate interests.

Exceptions

In the absence of an adequacy decision, including binding corporate rules, for the transfer of personal data to a third country, or an international organisation, it shall take place only on one of the following conditions as permitted under Article 49 of the UK GDPR:

1. The data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers due to the absence of an adequacy decision and appropriate safeguards.
2. The transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request.
3. The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person.
4. The transfer is necessary for important reasons of public interest.
5. The transfer is necessary for the establishment, exercise or defence of legal claims.
6. The transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.
7. The transfer is made from a register intended by UK law to provide information to the public and which is open to consultation with legal conditions.

The UK Government maintains a list of countries deemed to provide an adequate level of protection for personal data, which is published by the Information Commissioner's Office (ICO). If Global Mediation Limited processes personal data subject to the EU GDPR, it will separately comply with the European Commission's adequacy decision.

Accountability

The GDPR states that the controller is not only responsible for ensuring compliance but for demonstrating that each processing operation complies with the requirements of the GDPR. As a result, controllers are required to keep all necessary documentation of all processing operations, and implement appropriate security measures. They are also responsible for completing Data Processing Impact Assessments (DPIAs), complying with requirements for prior notifications, or approval from supervisory authorities and ensuring a DPO is appointed if required.

Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

1. To make subject access requests regarding the nature of information held and to whom it has been disclosed
2. To prevent processing likely to cause damage or distress
3. To prevent processing for purposes of direct marketing
4. To be informed about the mechanics of automated decision-taking process that will significantly affect them
5. Not to have significant decisions that will affect them taken solely by automated process
6. To sue for compensation if they suffer damage by any contravention of the GDPR
7. To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data
8. To request the ICO to assess whether any provision of the GDPR has been contravened
9. The right for personal data to be provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller
10. The right to object to any automated profiling without consent

Data subjects may make data access requests as described in the Subject Access Requests procedure. This procedure also describes how Global Mediation Limited will ensure that its response to the data access request complies with the requirements of the Regulation.

Complaints

A Data Subject has the right to complain at any time to Global Mediation Limited if they have concerns about how their information is used. If they wish to lodge a complaint, this should be directed to the DPO following the complaints procedure using a complaint form supplied by Global Mediation Limited. A complaints form can be obtained by emailing clientservices@globalmediation.co.uk.

A Data Subject also has the option to complain directly to the Information Commissioner's Office: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF or by visiting the ICO website at www.ico.org.uk.

Consent

Global Mediation Limited understands 'consent' to mean that it has been explicitly and freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement, or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her. The consent of the data subject can be withdrawn at any time.

In addition, Global Mediation Limited understands 'consent' to mean that the data subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing. There must be some active communication between the parties which demonstrate active consent. Consent cannot be inferred from non- response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

Consent to process personal and sensitive data is obtained routinely by Global Mediation Limited using standard consent documents. This may be through a contract of employment or during induction.

Where Global Mediation Limited provides online services to children, parental, or custodial authorisation must be obtained. This requirement applies to children under the age of 16 (unless the Member State has made provision for a lower age limit — which may be no lower than 13).

Data security

All Global Mediation Limited Staff that are responsible for any personal data which Global Mediation Limited holds must keep it securely and ensure that it is not disclosed under any conditions to any third party unless that third party has been specifically authorised by Global Mediation Limited to receive that information and has entered into a confidentiality agreement.

All personal data should be accessible only to those who need to use it, and access may only be granted in line with the Access Control Policy. You should form a judgment based upon the sensitivity and value of the information in question, but personal data must be kept:

1. In a lockable room with controlled access; and/or
2. In a locked drawer or filing cabinet; and/or
3. If computerised, it must be password protected in line with the Access Control Policy
4. Stored on encrypted removable media in line with the Cryptographic Controls Policy.

Care must be taken to ensure that PC screens and terminals are not visible except to authorised Staff of Global Mediation Limited. All Staff must sign up to the E-mail & Internet Acceptable Usage Policy before they are given access to organisational information of any sort.

Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit [written] authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with [procedure reference].

Personal data may only be deleted or disposed of in line with the Retention of Records procedure. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste'. Hard drives of redundant PCs are to be removed and immediately destroyed (see A.8.3.2 and A.11.2.7).Because of the increased risk, all Staff must be specifically authorised to process data off-site.

Rights of access to data

Data subjects have the right to access any personal data (i.e. data about them) which is held by Global Mediation Limited in electronic format and manual records which form part of a relevant filing system. This includes the right to inspect confidential personal references received by Global Mediation Limited, and information obtained from third party organisations about that person. Subject Access Requests are dealt with as described in the Subject Access Request Procedure.

Disclosure of data

Global Mediation Limited must ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police. All Employees/Staff should exercise caution when asked to disclose personal data held on another individual to a third party [and will be required to attend specific training that enables them to deal effectively with any such risk]. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of Global Mediation Limited's business.

GDPR permits a number of exemptions where certain disclosure without consent is permitted, as long as the information is requested for one or more of the following purposes:

1. To safeguard national security
2. Prevention or detection of crime including the apprehension or prosecution of offenders
3. Assessment or collection of tax duty
4. Discharge of regulatory functions (includes health, safety and welfare of persons at work)

5. To prevent serious harm to a third party
6. To protect the vital interests of the individual - this refers to life and death situations.

All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the Data Protection Officer.

Retention and disposal of data

Personal data may not be retained for longer than it is required. Once a member of staff has left Global Mediation Limited, it may not be necessary to retain all the information held on them. Some data will be kept for longer periods than others. Global Mediation Limited's data retention and data disposal procedures will apply in all cases.

Disposal of records

Personal data must be disposed of in a way that protects the "rights and freedoms" of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) (see A.8.3.2 and A.11.2.7).

E-mail and internet privacy

The inappropriate use of e-mail and the Internet by employees, e.g. using the Internet for non-work purposes, can have significant consequences for our Organisation. This can be in terms of:

1. Embarrassment/damage to the Organisation's reputation
2. Loss of productivity
3. Increased risk of liability and legal action, e.g. for sexist or racist e-mails
4. Increased virus risk.

To avoid inappropriate usage, we have introduced security electronic safeguards. A firewall checks, guarantees and manages e-mail attachments. The Organisation has installed filtering software that searches e-mails for specific words or phrases, normally obscene or discriminatory, and monitors which websites our employees are accessing as well as filtering which types of websites our employees can access.

Acceptable use of e-mail and the internet

Please see the e-mail and Internet Acceptable Usage Policy.

In addition, the Organisation's employees will be kept fully informed about overall information security procedures and the importance of their role within these procedures. Similarly, manual filing systems are held in secure locations and only authorised employees can access them.

Responsibilities and review

The Managing Director has overall responsibility for the administration and implementation of the Organisation's Data Protection Policy.

Each Department Manager will assume authority for the compliance of the employees within their department.

This Policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 2018 and the GDPR.

The Data Protection Policy will, under normal circumstances, be managed and reviewed annually. The reviews to the Policy will be subject to scrutiny and, from time to time, updates and re-issues will be circulated.

However, the Policy will be reviewed sooner in the event of any one or more of the following:

1. Weakness in the Policy is highlighted
2. Weaknesses in hardware and software controls are identified
3. In case of new threat(s) or changed risks
4. Changes in legislative requirements
5. Changes in Government, company or other directives and requirements.

Date of issue:	15 July 2025
Date of next review:	15 July 2026
Name:	A Gersch
Signed:	

Get in touch

t: 0208 441 1355
e: info@globalmediation.co.uk

visit us:
Molteno House
302 Regents Park Road
London, N3 2JX

globalmediation.co.uk

global mediation