DATED 2023

BINDING CORPORATE RULES
CONTROLLER STANDARD
OF MARSH & MCLENNAN COMPANIES, INC.

January 2023

MarshMcLennan

CONTENTS

INTENTIONALLY LEFT BLANK

INTRODUCTION

This Controller Standard establishes the approach of the Company to the protection and management of European Personal Information globally by Group Members in the circumstances described below.

Group Members and their employees must comply with and respect this Controller Standard when processing personal information.

This Controller Standard does not replace any pre-existing contractual or other statutory data protection requirements that might apply.

Information about this Controller Standard is available through the Company website at http://www.mmc.com/privacy-statement.html. A list of the current Group Members can be accessed here: https://www.mmc.com/privacy-statement/bcr-entities.html.

"**BCR Standards**" means collectively this Controller Standard and the Binding Corporate Rules Processor Standard of Marsh & McLennan Companies, Inc.

"**Company**" means collectively Marsh & McLennan Companies, Inc. and the Group Members.

"**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.

"**Controller Standard**" means this Binding Corporate Rules Controller Standard.

"**Data Subject**" means the Individual to whom Personal Information relates.

"**Europe**" means the European Economic Area and Switzerland.

"**European Data Protection Law**" means the GDPR and any data protection law of a Member State of European Economic Area and Switzerland, including local legislation implementing the requirements of the GDPR, in each case as amended from time to time and including subordinate legislation.

"**European Personal Information**" means Personal Information which is subject to European Data Protection Law.

"**Exporting Entity**" means a Group Member established in Europe that is Processing European Personal Information as a controller and transferring such Personal Information to an Importing Entity under this Controller Standard.

"**GDPR**" means European Union (EU) Regulation 2016/679 (the General Data Protection Regulation).

"**Group Members**" means the group members who have acceded to the MMC Intra-Group Agreement as participating in the MMC BCR program.

"**Importing Entity**" means a Group Member established outside Europe receiving European Personal Information from an Exporting Entity under this Controller Standard.

"**Personal Information**" means any information relating to an identified or identifiable natural person (referred to as an "**Individual**" or "**Data Subject**" in this Controller Standard).

"**Processing/Processed/Process**" means any operation that the Company performs on Personal Information, whether manually or by automatic means. References to the 'collection', 'use' and 'transfer' of Personal Information are all elements of the definition of Processing.

"**Processor**" means the entity which Processes Personal Information on behalf of the Controller.

"**Profiling**" means any form of automated Processing consisting of the use of Personal Information to evaluate certain personal aspects relating to an Individual, in particular to analyse or predict aspects concerning that Individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

"**Supervisory Authority**" means an independent public authority established in a European jurisdiction which is responsible for monitoring the application of European Data Protection Law in order to protect the fundamental rights and freedoms of Individuals in relation to Processing.

"**Third Party**" means any entity which is not a Group Member.

1. BACKGROUND AND ACTIONS

1.1 What is Data Protection Law?

European Data Protection Law gives Individuals the right to control how their Personal Information is Processed. The Company's Processing of the European Personal Information of clients, employees and suppliers is covered and regulated by European Data Protection Law.

Under European Data Protection Law, when a company Processes Personal Information for its own purposes, it is deemed to be a Controller of that information and is therefore primarily responsible for meeting the legal data protection requirements. So, for example, where that company acts as an employer, it is the Controller of the Personal Information it Processes about its employees.

When, on the other hand, a company Processes information on behalf of another one (for example, to provide a service), it is deemed to be a Processor of the information and that other company, as the Controller, will be primarily responsible for meeting the legal data protection requirements.

1.2 How does European Data Protection Law affect the Company internationally?

European Data Protection Laws do not allow the transfer of European Personal Information to countries outside of Europe that in the view of the European Commission do not ensure an adequate level of data protection (known as "**adequate jurisdictions**"). Some of the countries in which the Company operates are not regarded by the European Commission as adequate jurisdictions. European Data Protection Laws also allow transfers of Personal Information to countries outside of Europe pursuant to the GDPR Chapter V, including adequacy decision pursuant to Article 45(3), appropriate safeguards pursuant to Article 46 including binding corporate rules or derogations pursuant to Article 49.

1.3 What is the Company doing about it?

The Company takes privacy seriously. The purpose of this Controller Standard is to set out a framework to satisfy the standards contained in European Data Protection Law. This framework will allow the Company to provide a level of protection that is equivalent to that which is guaranteed under European Data Protection Law for European Personal Information that is transferred from Exporting Entities to Importing Entities, or is subsequently transferred by an Importing Entity to another Importing Entity.

1.4 What Personal Information and Processing does this Controller Standard cover?

This Controller Standard applies to European Personal Information which is Processed by and transferred from an Exporting Entity and is Processed by:

- Group Members for their own purposes, acting as a Controller, in the course of:
    - interacting with and servicing: (i) prospective and existing clients; (ii) vendors, supplier management business partners and other Third Parties with whom Group Members interact; (iii) Company employees and employee family members/dependants/nominated emergency contacts; and (iv) plan participants or employees of, or Third Parties named in relation to clients: and
    - the administration and management of relations with the Individuals mentioned above; and
- Group Members as a Processor on behalf of another Group Member as a Controller.

European Personal Information Processed under this Controller Standard includes:

- in relation to prospective and existing **clients** or **employees**, **plan participants** or **employees of clients**: contact names; addresses; telephone numbers; email addresses; date of birth; national identifier; health information; details related to insurances or risks insured; payment information; information necessary for the provision of insurance or consulting products or services; information related to other services requested from or provided by the Group Members;
- in relation to **Third Parties named in relation to clients** (such as client employees, plan participants or customers of clients (for example, individuals named in insurance claims)): names; addresses; date of birth; national identifier; details of involvement in risks insured; information necessary for the provision of insurance products to clients;
- in relation to **employees** or **Individuals insured** (past, existing or prospective): names; addresses; gender; date of birth; details of next of kin; contact telephone numbers; email addresses; educational history and qualifications; previous job history; references; driving licence; passport information; photo; management metrics, appraisals and feedback; correspondence and internet use; bank account details; national identifier; health information (for sickness reporting purposes); salary and bonus details; benefit package; pension contribution details; travel details; expense details; information on membership of private health schemes; disciplinary information; criminal convictions data; trade union membership; racial or ethnic origin; religious or philosophical beliefs;

- in relation to **employee family members/dependants/nominated emergency contacts**: names; relationship to employee; contact information; and

- in relation to **contractors, suppliers, vendors, business partners and other third parties**: company contact information relating to suppliers including company names; contact names; professional addresses and telephone numbers; details of goods and services provided; national identifier; bank account and payment details; email address.

This Controller Standard applies to all Group Members and their employees worldwide. Group Members must comply with the separate Binding Corporate Rules Processor Standard when they process certain Personal Information as a Processor on behalf of a Third Party Controller. Some Group Members may act as both a Controller and a Processor to one or more Third Party Controllers and must therefore comply with this Controller Standard as well as the Binding Corporate Rules Processor Standard as appropriate.

1.5 Further information

Questions regarding the provisions of this Controller Standard, Individuals' rights arising under this Controller Standard or any other data protection issues should be sent to the Company at the following email address: MMCBCR@mmc.com, with the subject line: "BCR Question." The question will be forwarded to the appropriate person or department within the Company for consideration and response.

The Global Chief Privacy Officer ("**GCPO**") is responsible for verifying that all changes to this Controller Standard are notified in accordance with **Appendix 7**.

If an Individual is unhappy about the way in which the Company has Processed his or her Personal Information under this Controller Standard, he or she may bring the matter to the Company's attention by using the complaint handling procedures, set out in **Appendix 5**.

2. CONTROLLER OBLIGATIONS

There are three possible scenarios where Group Members act as a Controller:

(a) The Group Member receives European Personal Information directly from the Data Subject;

(b) The Group Member receives European Personal Information from another Controller (e.g., an employer) but subsequently establishes a direct relationship with the Data Subject;

(c) The Group Member receives European Personal Information about a Data Subject from another Controller (e.g., an employer) and does not at

any subsequent point establish a direct relationship with the Data Subject such that all interactions with the Data Subject occur solely via the other Controller.

The Controller Standard shall apply directly to Group Members in scenario 1 above. In scenario 2 some of the obligations may be met initially by the other Controller. In scenario 3, Group Members will take such steps as are appropriate in the circumstances to pass those obligations contractually to the other Controller with whom the Data Subjects interact.

The remainder of this Clause 2 addresses Group Members' obligations as follows:

- **Section A** addresses the basic principles of European Data Protection Law that a Group Member must observe when it Processes and transfers European Personal Information which is subject to this Controller Standard. Section A also includes the obligations with which Group Members must comply when they Process such Personal Information as a Processor on behalf of another Group Member.

- **Section B** summarises the commitments made by Group Members to the Supervisory Authorities in connection with this Controller Standard.

- **Section C** describes the Third Party beneficiary rights that Group Members have granted to individuals under Clause 2 of this Controller Standard.

SECTION A: BASIC PRINCIPLES

RULE 1 – PROCESSING EUROPEAN PERSONAL INFORMATION LAWFULLY

Rule 1A – the Company will comply with local privacy law where it exists.

The Company will comply with any applicable legislation relating to Personal Information (e.g. in Europe, European Data Protection Law) and will assure that where European Personal Information is Processed this is done in accordance with such local law.

Where this Controller Standard applies and:

- there is no applicable law or the law does not meet the standards set out by the Rules in this Controller Standard, the Company will Process European Personal Information in accordance with the Rules in this Controller Standard; and

- applicable data protection law requires a higher level of protection than is provided for in this Controller Standard, the higher level of protection will take precedence.

Rule 1B – the Company will ensure that its Processing of European Personal Information is fair and lawful and that a legal basis exists for the Processing of that Personal Information.

The Company will ensure that its Processing of European Personal Information is fair and lawful, and that a legal basis for Processing that Personal Information exists where required. Taking into account any specific provisions of a particular European or Member State law, Group Members will only Process European Personal Information Personal Information where:

- the Individual has given consent to the Processing of his or her Personal Information and that consent meets the required standards under European Data Protection Law;
- it is necessary for the performance of a contract to which the Individual is party, or in order to take steps at the request of the Individual before entering into a contract;
- it is necessary for compliance with a legal obligation to which the Group Member is subject where that legal obligation derives from European law or the law of a European Member State;
- it is necessary in order to protect the vital interests of the Individual or of another Individual where the Individual is physically or legally incapable of giving consent;
- it is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in a Group Member where that Processing is set out either under European law or the law of a European Member State to which the Group Member is subject; or
- it is necessary for the purposes of the legitimate interests pursued by a Group Member or by a Third Party, except where those interests are overridden by the interests or fundamental rights and freedoms of the Individual.

Where the Processing of European Personal Information relates to criminal convictions and offences or related security measures, Group Members will not carry out such Processing otherwise than under the control of official authority or when the Processing is authorised by European or Member State law that provides appropriate safeguards for the rights and freedoms of Individuals.

Rule 1C – special category Personal Information which is subject to European Data Protection Law will only be Processed by the Company where the Individual's explicit consent has been obtained unless the Company has an alternative legal basis for Processing.

Special category Personal Information is information relating to an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, or genetic or biometric data processed for the purpose of uniquely identifying an Individual.

Processing of special category Personal Information which is subject to European Data Protection Law is only permitted on certain grounds, for example, where the:

- Individual has given explicit consent to the Processing of any special category of Personal Information for one or more specified purposes, unless European Data Protection Law provides that the prohibition on Processing special category data may not be lifted by an Individual;
- Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of Company or of the Individual in the field of employment and social security and social protection law in so far as it is authorised by European or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and interests of Individuals;
- Processing is necessary in order to protect the vital interests of an Individual where that Individual is physically or legally incapable of giving consent;
- Processing relates to Personal Information that is manifestly made public by the Individual;
- Processing is necessary for the establishment, exercise or defence of legal claims;
- Processing is necessary for reasons of substantial public interest on the basis of European or Member State law provided that it is proportionate to the aim pursued, respects the essence of data protection and provides for suitable and specific measures to safeguard the fundamental rights and interests of the Individual;
- Processing is necessary for the purposes of preventive or occupational medicine for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment, or the management of health or social care systems and services on the basis of European or Member State law, provided that the Processing is undertaken by or under the responsibility of a professional subject to duties of confidentiality under European or Member State law or by rules established by national competent bodies;

- Processing is necessary for reasons of public health which provides for suitable and specific measures to safeguard the rights and freedoms of Individuals, in particular duties of professional confidentiality.

Rule 1D – the Company will assess the impact of any Processing of European Personal Information that will involve high risks to the rights and freedoms of Individuals.

Group Members will assess the necessity and proportionality of any new Processing of European Personal Information that involves high risks to the rights and freedoms of Individuals in accordance with the applicable privacy impact assessment processes, as amended and updated from time to time. In the event that the data protection impact assessment indicates that the Processing will result in a high risk to Individuals, Group Members may be required to consult the competent Supervisory Authorities prior to beginning Processing in the absence of measures taken to mitigate the risk.

RULE 2 – ASSURING TRANSPARENCY AND PROCESSING EUROPEAN PERSONAL INFORMATION FOR A KNOWN PURPOSE ONLY

Rule 2A – the Company will explain to individuals, at the time their European Personal Information is collected, how that information will be processed.

When the Company collects European Personal Information directly from Individuals it will assure that those Individuals are told (usually by means of a fair processing statement) how such Personal Information will be Processed. The fair processing statement shall include the information required by European Data Protection Law, including:

- the identity and contact details of the Controller, the data protection officer, the recipients, or classes of recipients, and the source and categories of information received from Third Parties;

- the purpose and legal basis for Processing, including an explanation about any Processing based on legitimate interests and any new or different compatible purposes;

- information about the safeguards in place to protect the Personal information when it is transferred internationally and how to obtain a copy of such safeguards. In the case of transfers of European Personal Information between an Exporting Entity and an Importing Entity based on this Controller Standard, the information provided will include reference to this Controller Standard and how to access it;

- the length of time for which the Personal Information will be retained, or the criteria applied to calculate this;

- details of Individuals' rights, including right of access, rectification, erasure, restriction, portability, where Processing is based on consent, the right to withdraw consent, and the right to complain to a Supervisory Authority;

- whether the provision of the information is a statutory or contractual requirement, and the consequences of the failure to provide Personal Information in such circumstances; and

- information about any Personal Information that is used for automated decision-making, including Profiling and at least in cases where such decisions produce legal effects concerning the Individual or similarly significantly affect the Individual, or are based on special categories of Personal Information, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the Individual.

The requirements of the local law where the European Personal Information is collected will determine whether any additional information has to be provided to Individuals at the time when personal data is obtained.

Where the Company obtains an Individual's European Personal Information from a source other than that Individual, for example from the Individual's employer the Company will provide the information outlined above to the Individual:

- within a reasonable period of time after the Personal Information is obtained, but at the latest within one month;

- if the Personal Information is to be Processed for communication with the Individual, at the latest at the time of the first communication to that Individual; or

- if the Personal Information is to be disclosed to a Third Party, no later than the time when the information is first disclosed.

There may be situations in which the Company collects European Personal Information from another Controller, rather than directly from the Individual, and does not have a direct relationship with the Individual (e.g. where a Group Member provides actuarial or insurance services to a client). In such cases the Company will take such steps as are appropriate in the circumstances to obtain a commitment from the other Controller to provide the appropriate information to the Individual. In such cases the Group Member may provide to the other Controller the requisite fair processing statement so that it may share that statement with the relevant Individuals, or include appropriate terms in the service agreements with the other Controller which require the other Controller to provide fair processing information to Individuals which explains how their information may be shared with a Group Member.

The Company will follow this Rule 2A unless there is a legitimate basis for not doing so (for example, where it is necessary to safeguard national security or defence, for the prevention or detection of crime, taxation purposes, legal proceedings, or where otherwise permitted by European Data Protection Law).

Rule 2B – the Company will only Process European Personal Information for those purposes which are disclosed to Individuals, or which are within their expectations as relevant to the products or services being offered.

The Company will identify and make known the purposes for which European Personal Information will be Processed (including the secondary uses and disclosures of the information) in accordance with Rule 2A

Rule 2C – the Company may only Process European Personal Information for an undisclosed or new purpose if the Company has a legitimate basis for doing so, consistent with European Data Protection Law.

If the Company collects European Personal Information for a specified purpose in accordance with Rule 2B and subsequently the Company wishes to process that Personal Information for a different or new purpose, it will not further Process the information in a way incompatible with the purpose for which it was collected.

In certain cases, for example, where Processing special categories of Personal Information, the individual's explicit consent (in the case of special categories of personal information) to the new Processing may be necessary.

RULE 3 – ASSURING DATA QUALITY

Rule 3A – the Company will keep European Personal Information accurate and up to date.

In order to verify that the European Personal Information held by the Company is accurate and up to date, the Company actively encourages Individuals (or other Controllers interacting with the Company on behalf of such Individuals) to inform the Company when their Personal Information changes. The Company will take every reasonable step to ensure that European Personal Information that are inaccurate, having regard to the purposes for which they are Processed, are erased or rectified without delay.

Rule 3B – the Company will only keep European Personal Information for as long as is required for the purposes for which it is collected and further Processed.

The Company will comply with the its record retention policies and procedures as revised and updated from time to time and delete European Personal Information that no longer needs to be kept under the Company's record retention policies and the applicable retention schedules.

Rule 3C – the Company will only Process European Personal Information which is appropriate, relevant and limited to what is necessary in relation to the purposes for which they are Processed.

The Company will identify the appropriate and relevant amount of European Personal Information that is required in order to properly fulfil its purposes and strive to avoid collecting Personal Information beyond those requirements.

RULE 4 – TAKING APPROPRIATE SECURITY MEASURES

Rule 4A – the Company will follow its IT security policies.

The Company will implement appropriate technical and organisational measures to protect European Personal Information against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access, in particular where Processing involves transmission of Personal Information over a network. To this end, the Company will follow its IT security policies as revised and updated from time to time, together with any other security procedures relevant to a Group Member or function.

Rule 4B – the Company will adhere to its data breach notification processes.

The Company will adhere to its data breach notification processes (as revised and updated from time to time) which set out the process which must be followed in the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, European Personal Information transmitted, stored or otherwise processed (a "**Data Protection Breach**").

In particular, in the event of a Data Protection Breach, the relevant Group Member will, without undue delay, notify:

- the GCPO and/or the MMC Head of Privacy, EMEA ("**Head of Privacy**");
- Marsh & McLennan Ireland Limited; and
- the competent Supervisory Authority, unless the Data Protection Breach is unlikely to result in a risk to the rights and freedoms of Individuals.

Individuals will be notified in cases where the Data Protection Breach is likely to result in a high risk to their rights and freedoms unless such notification is not required under European Data Protection Law.

The GCPO and/or the Head of Privacy will record Data Protection Breaches suffered by Group Members, the effects of such incidents and the remedial action taken in a Data Protection Breach report which will be available to a competent Supervisory Authority on request.

Rule 4C – the Company will assure that providers of services to the Company also adopt appropriate and equivalent security measures.

Where a provider of a service (acting as a processor) to any of the Group Members has access to European Personal Information (e.g. a payroll provider), the Company will impose on the service provider contractual obligations evidenced in writing which meet the requirements of European Data Protection Law. Such obligations shall require, for example, the service provider to have in place the appropriate technical and organisational security measures to safeguard the personal information and to act only on the Company's instructions when Processing that information.

Rule 4D – Where one Group Member provides a service as a Processor to a Controller Group Member, the Group Members will put in place appropriate contractual provisions and security measures as required by European Data Protection Law.

Where a Group Member (Entity A) Processes European Personal Information as a Processor on behalf of a Group Member which is a Controller (Entity B), Entity A will:

- act only on the documented instructions of Entity B. Such instructions may be provided by Entity B by means of a completed Processing Schedule (as set out in Appendix 8); and
- comply with the obligations set out in Part 2 of the Processing Schedule, or as appropriate, a contract or legal act entered into between Entity A and Entity B in relation to such Processing which is consistent with European Data Protection Law in so far as it relates to the engagement of a Processor.

RULE 5 – HONOURING INDIVIDUALS' RIGHTS

Rule 5A – the Company will adhere to the BCR Individuals' Rights Request Procedure when dealing with queries or requests made by individuals in connection with their European Personal Information.

Individuals are entitled (by submitting a request to the Company through the BCR Individuals' Rights Request Procedure) to be supplied with a copy of the European Personal Information held about them (including information held in both electronic and paper records), together with certain other details such as their rights in relation to the Personal Information. This is known as the right of subject access in European Data Protection Law. The Company will follow the steps set out in the BCR Individuals' Rights Request Procedure (see, **Appendix 1**) when dealing with requests from Individuals for access to their European Personal Information.

Rule 5B – the Company will deal with requests to rectify, erase, restrict, port or complete European Personal Information, or objections to the

Processing of that Personal Information in accordance with the BCR Individuals' Rights Request Procedure.

On request, individuals are entitled in certain circumstances, as prescribed by European Data Protection Law, to:

- request rectification, completion, erasure, or restriction, as appropriate of their Personal Information;
- exercise their right to data portability in relation to their Personal Information; and/or
- object to the Processing of their Personal Information, including Processing for direct marketing purposes and to Profiling to the extent that it is related to such marketing.

The Company will follow the steps set out in the BCR Individuals' Rights Request Procedure (see **Appendix 1**) in such circumstances.

RULE 6 – ASSURING ADEQUATE PROTECTION FOR TRANSFERS AND ONWARD TRANSFERS

Rule 6 – the Company will not transfer European Personal Information to Third Parties outside Europe without assuring adequate protection for the information in accordance with the standards set out by this Controller Standard.

The Company will assure that any transfers and onward transfers of European Personal Information to Third Parties outside Europe will occur under appropriate steps in order to ensure that adequate protection will be provided in the third country by way of an adequacy decision pursuant to Article 45(3), or of Appropriate Safeguards pursuant to Article 46, including Binding Corporate Rules or Article 49 Derogations, as required by European Data Protection Law. These steps may include:

- signing the appropriate contractual clauses or an equivalent data transfer agreement;
- confirming that the Third Party is located in a country which the European Commission has found to offer an adequate level of protection for the European Personal Information transferred; or
- ensuring that the transfer is necessary for: i) the performance of a contract between the Individual and the transferring Group Member or for the implementation of pre-contractual measures taken at the Individual's request; ii) the conclusion or performance of a contract concluded in the interest of the Individual between the transferring Group Member and another party; iii) important reasons of public interest as laid down by European Union or Member State law; iv) the establishment, exercise or

defence of legal claims; or v) the protection of the vital interests of the Individual or of another Individual and where the Individual is incapable of giving consent; or vi) obtaining the explicit consent of the Individual, after having informed the Individual of the possible risks of such transfers for the Individual due to the absence of an adequacy decision and appropriate safeguards.

RULE 7 – LEGITIMISING DIRECT MARKETING

Rule 7 – The Company will allow Individuals to opt-out of receiving marketing information.

Individuals will honour all such opt-out requests.

RULE 8 – AUTOMATED INDIVIDUAL DECISIONS

Rule 8 – The Company will respect the right of Individuals not to be subject to a decision made as a result of the Processing of European Personal Information by automated means (including Profiling) which has a legal or similarly significant effect on them, unless the Processing is permitted under European Data Protection Law and the Company has put in place necessary measures to protect the legitimate interests of Individuals.

Under European Data Protection Law no evaluation of or decision about an Individual which significantly affects them can be based solely on the automated Processing of Personal Information unless;

- the Processing is authorised under European Data Protection Law;
- the decision is necessary for entering into a contract between the Individual and the Group Member; or
- the Individual has given their explicit consent,

and in such cases the Company will comply with its obligations to notify data subjects in accordance with Rule 2A and put in place measures to protect the rights and freedoms and legitimate interests of Individuals, such as the right for an Individual to obtain human intervention in the decision, to express his or her point of view and to contest the decision.

SECTION B: PRACTICAL COMMITMENTS

RULE 9 – COMPLIANCE AND ACCOUNTABILITY

Rule 9A – Group Members will be responsible for and able to demonstrate compliance with this Controller Standard and the Company will have appropriate resources to oversee compliance with this Controller Standard throughout the Group Members.

The Company has appointed its GCPO as the person to oversee compliance with this Controller Standard supported by a network of privacy leaders and privacy coordinators in the various Group Members' countries (collectively referred to as the "**Global Privacy Network**"), all of whom together are responsible for overseeing and enabling compliance with this Controller Standard on a day to day basis. A summary of the roles and responsibilities of the Company's privacy team is set out in **Appendix 2**.

Rule 9B – The Company will implement appropriate technical and organisational measures to enable and facilitate compliance with the Controller Standard in practice.

Taking into account the state of the art and cost of implementation, and the scope, nature, context and purposes of the processing, the Company will implement appropriate technical and organisational measures which meet the principles of data protection by design and by default as required by European Data Protection Law. The Company will integrate such measures into the processing when determining the means of the processing, and the time of processing itself to facilitate the protection of European Personal Information being processed, and in order to ensure that, by default, only personal information which is necessary for each specific purpose of the processing is processed.

Rule 9C – Group Members processing European Personal Information will maintain a written (which includes in electronic form) record of their Processing activities and make that record available to competent Supervisory Authorities on request.

The data processing records maintained by Group Members will contain:

- the Group Member's name and contact details and where applicable, details of the data protection officer;
- the purposes for which the European Personal Information is Processed;
- a description of the categories of individuals about whom the European Personal Information is Processed and the European Personal Information Processed;
- the categories of recipients to whom the European Personal Information has been or will be disclosed including recipients in third countries or international organisations;
- details of the third country or countries to which the Personal Information is transferred including the identification of that third country or international organisation and the documentation of suitable safeguards in the event of transfers under the second subparagraph of Article 49(1) of the GDPR;

- where possible, the period for which the European Personal Information will be retained; and
- where possible, a general description of the technical and organisational security measures used to protect the European Personal Information.

RULE 10 – TRAINING

Rule 10 – The Company will provide appropriate training to employees who have permanent or regular access to European Personal Information, who are involved in the Processing of European Personal Information or in the development of tools used to Process such Personal Information in accordance with the Privacy Training Requirements Protocol in Appendix 3.

RULE 11 – AUDIT

Rule 11 – The Company will comply with the Audit Protocol set out in Appendix 4.

RULE 12 – COMPLAINT HANDLING

Rule 12 – The Company will comply with the Complaints Handling Protocol – External (set out in Appendix 5A) and the Complaints Handling Protocol – Internal (set out in Appendix 5B).

RULE 13 – COOPERATION WITH SUPERVISORY AUTHORITIES

Rule 13 – The Company will comply with the Co-operation Procedure set out in Appendix 6.

RULE 14 – UPDATE OF THE RULES

Rule 14 – The Company will comply with the Updating Procedure set out in Appendix 7.

RULE 15 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE CONTROLLER STANDARD

Rule 15A – The Company will carry out a transfer impact assessment before making transfers under the Controller Standard.

The Company will carry out a transfer impact assessment to assess if the legislation applicable to Importing Entities prevents them from fulfilling their obligations under the Controller Standard or has a substantial effect on the guarantees provided under the Controller Standard before making transfers of European Personal Information under the Controller Standard. Any laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR, are not in

contradiction with this Controller Standard. The transfer impact assessment must take into account:

- the specific circumstances of the transfer such as the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred European Personal Information; the economic sector in which the transfer occurs; and the storage location of the data transferred;

- the laws and practices of the third country (including the possibility of legal access requests by public authorities) relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards; and

- any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under this Controller Standard, including measures applied during transmission and to the processing of the personal data in the country of destination.

If it is assessed that any safeguards in addition to those envisaged under the Controller Standard should be put in place, Marsh & McLennan Ireland Limited, the GCPO and the Head of Privacy will be informed and involved in the determination of those additional safeguards.

Such transfer impact assessment must be appropriately documented, including details of any supplementary measures selected and implemented, as applicable, and will be made available to competent Supervisory Authorities upon request.

After carrying out a transfer impact assessment, Group Members will be informed that the assessment has been carried out and:

- of the results of the transfer impact assessment so that the identified additional safeguards are applied; or

- where additional safeguards could not be put in place, that the relevant transfers will be suspended or ended. If the transfers are suspended, any European Personal Information transferred prior to the suspension will be, at the request of the Exporting Entity, destroyed or returned to the Exporting Entity. In any event, the Exporting Entity can choose to end the transfer following such suspension.

Rule 15B – The Company agrees that where a Group Member believes that the legislation applicable to it prevents it from fulfilling its obligations under the Controller Standard or such legislation has a substantial effect on the guarantees provided by the Controller Standard, such Group Member will promptly inform Marsh & McLennan Ireland Limited as

applicable and the GCPO, unless otherwise prohibited by law or a law enforcement authority.

In addition to the above:

- Importing Entities will notify Exporting Entities where there is a change in the laws of the third country which could affect the results of the initial transfer impact assessment carried out in accordance with Rule 15A; and

- Exporting Entities will monitor, on an ongoing basis, any developments in the third countries which could affect the results of the initial transfer impact assessment carried out in accordance with Rule 15A.

- Upon verification of such notification, the Exporting Entity, along with Marsh & McLennan Ireland Limited, the GCPO and the Head of Privacy, commit to promptly identify appropriate measures (e.g., technical or organisational measures to ensure security and confidentiality), as needed, to be adopted by the Exporting Entity and/or the Importing Entity in order to enable them to fulfil their obligations under this Controller Standard. The same applies if an Exporting Entity has reason to believe that an Importing Entity can no longer fulfil its obligations under this Controller Standard.

- Where the Exporting Entity (along with Marsh & McLennan Ireland Limited, the GCPO and the Head of Privacy), assesses that no appropriate safeguards for the transfer or set of transfers can be ensured or if instructed by the competent Supervisory Authority, it commits to suspend the transfer or set of transfers.

Rule 15C – The Company agrees that where there is a conflict between the legislation applicable to a Group Member and this Controller Standard, the GCPO will make a decision on the action to be taken and consult the Supervisory Authority with competent jurisdiction.

Rule 15D – Where the Company receives a legally binding request from a law enforcement agency or state security body for disclosure of European Personal Information transferred outside Europe under this Controller Standard, the Company will, unless prohibited from doing so, put the request on hold and promptly notify the competent Supervisory Authority.

Where the Company receives a legally binding request for disclosure of Personal Information transferred outside Europe under this Controller Standard and is prohibited–from putting the request on hold and/or from notifying the competent Supervisory Authorities, the Company will:

- use its best efforts to obtain a waiver of this prohibition in order to communicate as much information as it can and as soon as possible to the competent Supervisory Authorities; and

- demonstrate to the competent Supervisory Authorities the steps it followed to deal with the request in accordance with this Controller Standard.

Where the Company is not able to notify the competent Supervisory Authorities, the Company will provide to the competent Supervisory Authorities on an annual basis general information about the nature and number of such requests that it receives and will ensure that any transfers that it makes to a public authority are not massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

1. The Company agrees that Individuals whose European Personal Information is Processed in Europe by an **Exporting Entity** as a controller and transferred to an Importing Entity benefit from certain rights to enforce compliance with Rules 1B and 1C, 2, 3, 4, 5, 6, 7, 8, 9B, 12, 13, and 15, the right to easy access to information to which such Individuals are entitled regarding this Controller Standard and the provisions in sub-sections 1, 2 and 3 of this Section C granting third-party beneficiary rights and setting the liability and jurisdiction rules under the Controller Standard by:

   - **making a complaint** to: i) a European Group Member in accordance with the External Complaint Handling Procedure in Appendix 5A or the Internal Complaint Handling Procedure in Appendix 5B, as appropriate; and/or ii) a competent Supervisory Authority in the jurisdiction in which the alleged infringement took place, or in which the Individual works or habitually resides; and/or

   - **bringing proceedings against the Exporting Entity** before the competent courts in Europe in: i) the jurisdiction of the Exporting Entity; ii) a Member State in which the Exporting Entity has an establishment; or iii) the Member State in which the Individual has their habitual residence.

2. In the event that the Exporting Entity is established in Europe, the individuals referred to in sub-section 1 of this Section C may also seek appropriate redress from the Exporting Entity which agrees to take the necessary action to remedy of any breach of the provisions or any of them listed in sub-section 1 of this Section C by any Importing Entity and, where appropriate, receive compensation from the Exporting Entity in accordance with the determination of a court or other competent authority for any damage, whether material or non-material, suffered as a result of a breach of the provisions or any of them listed in sub-section 1 of this Section C by a Group Member.

3. If a claim is made in which any such Individual has suffered damage where that Individual can demonstrate that it is likely that the damage has occurred because a breach of this Controller Standard the Company has agreed that the burden of proof to show that an Importing Entity is not responsible for the

breach, or that no such breach took place, will rest with the Exporting Entity as described in sub-section 2 or 3 of this Section C.

4. In the event that the Exporting Entity has factually disappeared, ceased to exist in law or has become insolvent, the Individual may enforce the provisions referred to under this Section C against Marsh & McLennan Ireland Limited as if Marsh & McLennan Ireland Limited were that Exporting Entity.

5. The information to which Individuals are entitled regarding this Controller Standard is available on http://www.mmc.com/privacy-statement.html. A list of the current Group Members can be accessed here: https://www.mmc.com/privacy-statement/bcr-entities.html.

3. APPENDICES

APPENDIX 1 - BCR INDIVIDUALS' RIGHTS REQUEST PROCEDURE

1. BACKGROUND

1.1 The Company has adopted the BCR Standards to safeguard European Personal Information transferred between Group Members.

1.2 The BCR Standards require approval from the Supervisory Authorities in the European Member States from which the European Person Information is transferred. The Supervisory Authorities require the Company to maintain a process to address requests from individuals relating to the European Personal Information processed under the BCR Standards and to satisfy certain conditions in so doing. This document describes how the Company meets such requirements.

2. INTRODUCTION

2.1 When the Company processes European Personal Information for its own purposes, the Company is deemed to be a controller of that information and is therefore primarily responsible for meeting the requirements of European Data Protection Law.

2.2 Where the Company acts as a controller, individuals whose European Personal Information is processed by the Company have the right to:

(a) be informed whether any such European Personal Information is being processed by the Company and to a copy of that information (this is known as the right of "**subject access**"); and

(b) rectify, erase, restrict, or complete their European Personal Information, to data portability, not to be subject to certain decisions based solely on automated processing; and/or to object to the processing of their European Personal Information.

2.3 In addition, all individuals whose European Personal Information is processed by the Company acting as controller, and transferred to another Group Member outside Europe will also benefit from the rights described in section 2.2 above.

2.4 This Procedure explains how the Company deals with requests relating to European Personal Information which fall into the categories in sections 2.2 and 2.3 above (referred to as "**valid request**" in this Procedure). Where applicable European Data Protection Law differs from this Procedure, the European Data Protection Law will prevail.

2.5 Information about how individuals may exercise the rights described in this Procedure is set out in the fair processing statements provided to individuals by

the Company. Individuals may also contact the Head of Privacy to exercise these rights.

3. INDIVIDUALS' RIGHTS

3.1 An individual making a valid request to the Company is entitled to:

(a) be informed whether the Company is processing European Personal Information about that person;

(b) be given a description of:

(i) the purposes for which the European Personal Information is being processed and the categories of European Personal Information concerned;

(ii) the recipients or categories of recipient to whom the information is, or may be, disclosed by the Company, including recipients located outside Europe;

(iii) the safeguards in place where European Personal Information is transferred from Europe to a third country;

(iv) the logic involved (to the extent required by applicable law), significance, and consequences of any processing undertaken by automatic means, including profiling;

(c) be advised, where possible, about the period for which the European Personal Information will be stored, or the criteria used to determine that period;

(d) be informed about the rights to rectification, erasure, objection and to complain to a Supervisory Authority;

(e) be given details as to the source of the European Personal Information if it was not collected from the individual;

(f) where the valid request is for subject access, receive a copy of their European Personal Information held by the Company. If the request is made by email, the information shall be provided via email, unless the individual making the request indicates otherwise;

(g) where the valid request is for data portability made by an individual who has provided their European Personal Information to the Company, receive that information in a structured, commonly used and machine-readable format and, if required and technically feasible, have it transmitted to another controller;

(h) not be subject to a decision based solely on automated processing, including profiling, which produces legal or similar significant effects;

(i) require the rectification, erasure, restriction, portability or completion of their European Personal Information; and/or

(j) object to the processing of their European Personal Information.

4. PROCESS

4.1 Requests from individuals relating to the rights described in section 2.2 and 2.3 above may be made in writing, which can include an email message. Where requests are made by email, they should be emailed to mmcbcr@mmc.com with the subject line: "BCR Access Request." However, the request does not have to specifically state that it is a BCR request or make reference to European Data Protection Law in order to qualify as a valid request. Where an oral request is made, the Company will document the request and provide a copy to the individual making the request before dealing with it.

4.2 When the Company is a controller of the European Personal Information which is the subject of a valid request:

(a) If the Company receives a request from an individual relating to the rights described in section 2.2, it shall be passed to the Head of Privacy, Global Chief Privacy Officer ("GCPO") or a member of the Global Privacy Network immediately upon receipt, indicating the date on which it was received together with any other information which may assist the Global Privacy Network member to deal with the request.

(b) The Global Privacy Network member will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required.

(c) The Global Privacy Network member will then contact the individual in writing to confirm receipt of the valid request, seek confirmation of identity or further information, if required to comply with the request, or decline the request if one of the below exemptions to the relevant right applies.

5. EXEMPTIONS TO THE RIGHT OF SUBJECT ACCESS FOR REQUESTS MADE TO THE COMPANY AS A CONTROLLER

5.1 A valid request may be refused by the Company on the following grounds:

(a) where the request is made to a European Group Member and relates to the use or collection of European Personal Information by that Group Member, if:

(i) the refusal to provide the information is consistent with the data protection law within the jurisdiction in which that Group Member is located; or

(ii) that Group Member demonstrates that the request is manifestly unfounded or excessive; and

(iii) the Group Member informs the individual of the refusal of the request within one month of the receipt of the request, together with the reasons for not taking action and the individual's right to complain to a supervisory authority or seek a judicial remedy in relation to the refusal; or

(b) where the request is made to a non-European Group Member, the relevant non-European Group Member may refuse the request if the grounds for such refusal are consistent with the data protection law of the European jurisdiction from which the European Personal Information was transferred.

6. THE COMPANY'S SEARCH AND RESPONSE TO A VALID REQUEST

6.1 The Company must deal with a valid request without undue delay and in any event within one month of its receipt. The Company may extend this period by up to two further months if necessary if the request is complex or where there are numerous requests. Where the period in which it will deal with a valid request is extended, the Company will inform the individual of:

(a) the extension; and

(b) their right to lodge a complaint with a competent Supervisory Authority or seek a judicial review,

within one month of receipt of their request, together with the reasons for the delay.

6.2 The Global Privacy Network member will arrange a search of the relevant applications pertaining to the request.

6.3 The Global Privacy Network member may refer any complex cases to the Head of Privacy, GCPO, or, if the matter originated with the Head of Privacy or GCPO, to the General Counsel and/or Chief Risk & Compliance Officer of the relevant Group Member for advice, particularly where the request includes information relating to third parties or where the release of European Personal Information may prejudice commercial confidentiality or legal proceedings.

6.4 Where the valid request is a request for subject access, the information requested will be collated by the Global Privacy Network member into a readily understandable format (internal codes or identification numbers used at the

Company that correspond to European Personal Information shall be translated before being disclosed). A cover letter will be prepared by the Global Privacy Network member that includes information required to be provided in response to the request.

6.5 Where the valid request is a request for data portability, the European Personal Information requested will be collated by the Global Privacy Network member into a structured, commonly used and machine-readable format and, at the request of the individual and where technically feasible, transmitted to another controller.

6.6 If the valid request is for the rectification, erasure, restriction or completion of European Personal Information, an objection to the processing of an individual's European Personal Information or relates to the right not to be subject to automated decision-making, such a request must be considered and dealt with as appropriate by the Company/a Global Privacy Network member.

6.7 If the valid request is advising of a change or any inaccuracy in an individual's European Personal Information, such information must be rectified or updated accordingly and without undue delay if the Company/a Global Privacy Network member is satisfied that there is a legitimate basis for doing so.

6.8 If the valid request is to erase that individual's European Personal Information in accordance with the provisions of applicable data protection law, the matter will be assessed by the Company/a Global Privacy Network member. Where the processing undertaken by the Company is required by law or is necessary for the exercising of the right of freedom of expression and information, the request will not be regarded as valid.

6.9 When, pursuant to a valid request, the Company erases, anonymises, updates, or corrects European Personal Information, the Company will notify other Group Members or any processor to whom the relevant European Personal Information has been disclosed accordingly so that they can also update their records.

6.10 The Company will not charge a fee for responding to requests made by individuals under this Procedure unless, in the reasonable opinion of the Head of Privacy/a Global Privacy Network member, the Company is able to demonstrate that the request is manifestly unfounded or excessive, in which case the Company may charge a reasonable fee.

7. REQUESTS MADE TO THE COMPANY WHERE THE COMPANY IS A PROCESSOR OF THE PERSONAL INFORMATION

7.1 When the Company processes information on behalf of a Client (for example, to provide a service) or other controllers, it is deemed to be a processor of the information. This means that its controller retains the responsibility to comply with European Data Protection Law and will be primarily responsible for

handling requests from individuals relating to their rights under European Data Protection Law.

7.2 Certain data protection obligations are passed to the Company in the contracts it has with its Clients and it must act in accordance with the instructions of its Clients and undertake any reasonably necessary measures to enable its Clients to comply with their duty to respect the rights of individuals. This means that if any Group Member receives a request in its capacity as a processor for a Client under the Processor Standard, that Group Member must transfer such request promptly to the relevant Client, unless authorised (or required) by the Client to respond to the request.

All queries relating to this Procedure are to be addressed to a member of the Global Privacy Network or sent to mmcbcr@mmc.com with the subject line: "BCR Access Request Question."

APPENDIX 2 - COMPLIANCE STRUCTURE

MARSH & MCLENNAN GLOBAL PRIVACY NETWORK

At the head of the Marsh & McLennan ("**MMC**") Global Privacy Network stands the GCPO who reports directly to MMC's Deputy General Counsel, Chief Compliance Officer, and Corporate Secretary ("**MMC CCO**"), and MMC's Chief Information Officer ("**MMC CIO**").

The Global Privacy Network has four components:

1. MMC Privacy and Information Governance Committee.
2. MMC Privacy Senior Leadership Team.
3. MMC Global Privacy Advisory Group.
4. Regional Privacy Councils.

1. MMC Privacy and Information Governance Committee

This group includes the MMC CIO, MMC CCO, GCPO and Head of Privacy at the MMC level, the Chief Operating Officer and Chief Information Officer from each of the four businesses of MMC (Marsh, Mercer, Guy Carpenter and Oliver Wyman), as well as the privacy leaders at the two larger businesses (Marsh and Mercer). The group meets monthly and discusses operational and technological implications of global privacy regulations as well as matters related to information governance.

2. MMC Privacy Senior Leadership Team

This newly formed group includes the GCPO, Head of Privacy and Senior Privacy Counsel at the MMC level and the privacy leaders from each of the four businesses of MMC. The group meets monthly and discusses privacy strategy and various operational elements related to the privacy program initiatives.

3. MMC Global Privacy Advisory Group.

The Global Privacy Advisory Group comprises the Privacy Senior Leadership Team as well as additional members from the privacy teams across the Group Members.

The responsibilities of the MMC Global Advisory Group are:

a. Privacy Program Development.

Assist the GCPO in identifying legal and regulatory requirements, client contractual obligations and / or expectations, obligations under Company policies as well as privacy risks identified through industry reports on external threats, and internal sources. Once identified, the MMC Global Advisory Group will suggest appropriate risk mitigation controls and strategies to manage those risks, and suggest a prioritization of the related privacy projects and initiatives. This information then formulates the MMC Privacy Strategic Plan which is

presented to the MMC Deputy General Counsel, Chief Compliance Officer, and Corporate Secretary, and MMC's Chief Information Officer on an annual basis.

b. Privacy Program Oversight.

The MMC Global Advisory Group members assist the GCPO in overseeing the execution of the MMC Privacy Strategic Plan by:
a) Engaging their businesses.
b) Identifying emerging risks and recommending mitigation strategies.
c) Monitoring plan implementation and providing updates to the core team.
d) Establishing ways to assess overall effectiveness of the MMC Privacy Strategic Plan.

c. Policies and Procedures.

The MMC Global Advisory Group will assist in harmonizing existing policies to create consistent policies throughout the Company and identify areas where new policies and procedures are deemed needed.

MMC Privacy Advisory Group Meetings: the MMC Privacy Advisory Group meets monthly. Standard Agenda items are:

- Legal and Regulatory developments / new risk
- Project Status
- Incidents of note
- Member escalations

Additional agenda items are added as needed.

4. Regional Privacy Councils

There are 3 regional privacy councils in place:

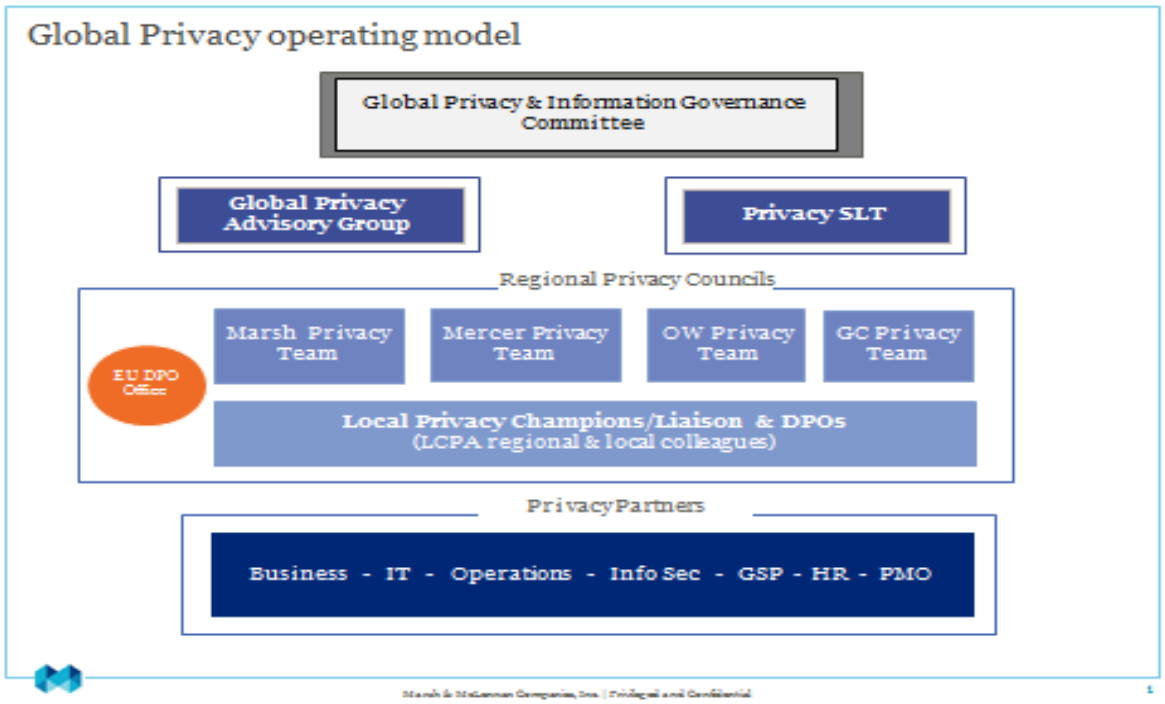
- EMEA
- Americas
- Asia Pacific

Participants in the core team meetings are colleagues from Legal, Compliance and Public Affairs who represent all MMC entities.

Scheduled Meetings: the Regional Privacy Councils meet quarterly. Standard Agenda items are:

- New legal developments in the region
- Status of key privacy projects
- Update on other initiatives of interest

Additional agenda items are added as needed.



Global Privacy – Roles and Responsibilities

Global Chief Privacy Officer (GCPO)

Reporting directly to the Board of Directors, the GCPO:

- defines the privacy strategy and key elements of the global privacy programme for the Company;
- oversees the Privacy Network;
- oversees the development, implementation and maintenance of the global privacy programme, including the Binding Corporate Rules;
- acts as incident leader for personal data breaches and privacy incidents;
- defines key themes for internal and external privacy communications;
- coordinates privacy compliance obligations across the organisation through management of privacy governance groups e.g. privacy committees, and direct engagement with personal information processing operations;
- assists with resource coordination and risk evaluation and assessing;
- acts as contact for and co-operates with Supervisory Authorities;
- enables the DPO to carry out its responsibilities.

Head of Privacy

Reporting directly to the GCPO, the Head of Privacy:

- oversees the development, implementation and ongoing maintenance of the data protection program that meets evolving GDPR requirements and the wider privacy program including overseeing the management, maintenance of and compliance with the Binding Corporate Rules;
- act as the lead privacy legal adviser for MMC Corporate Services, issuing guidance and alerts, and offering and delivering training;
- monitors and assesses privacy regulatory developments for the EMEA region;
- reviews and advises on DPIAs;
- advises on and manages suspected and actual data breaches and privacy incidents;
- acts as the contact for and co-operates with Supervisory Authorities;
- helps to manage data breach and privacy incidents;
- helps to manage and implement tools and processes to address evolving privacy and data protection risks inherent in the Company's EMEA operations;
- participates in new business initiatives and product development activities across EMEA.

Privacy Leaders

The Privacy Leaders:

- oversee and monitor compliance with the data protection program;
- advise employees and Local Privacy Champions of privacy obligations and compliance;
- monitor and escalate any suspected or actual data breaches and privacy incidents to the relevant business incident leaders, DPO and GCPO;
- assist with and support internal staff training in respect of privacy and data protection;
- conduct, assist with and manage DPIAs;
- manage, monitor and ensure compliance in respect of requests from data subjects;
- support internal and external data privacy communications.

Local Privacy Champions

The Local Privacy Champions:

- support Privacy Leaders in overseeing and monitoring compliance with the data protection program;

- act as a first point of contact for employees who seek advice in respect of privacy obligations and compliance and where necessary and appropriate escalate queries to Privacy Leaders;
- supports Privacy Leaders in monitoring and escalating any suspected or actual data breaches;
- assist with and support Privacy Leaders in providing internal staff training in respect of privacy and data protection;
- support Privacy Leaders to conduct, assist with and manage DPIAs;
- assist and support Privacy Leaders in managing, monitoring, responding to and ensuring compliance in respect of requests from data subjects;
- support internal and external data privacy communications.

Data Protection Officer

The Company's Data Protection Officer (as defined under the GDPR) is responsible for:

- informing and advising the controller or the processor and the employees who carry out processing of their obligations pursuant to the GDPR and to other Union or Member State data protection provisions;
- monitoring compliance with the GDPR, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- providing advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;
- cooperating with the supervisory authority;
- acting as the contact for data subjects in relation to requests relating to data subject rights and advising wider business functions on their obligations in responding to such requests;
- acting as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter;
- providing regular updates to senior management, risk committees and oversight committee.

APPENDIX 3 - PRIVACY TRAINING REQUIREMENTS PROTOCOL

1. BACKGROUND

1.1 The purpose of the BCR Standards is to provide a framework for the transfer of European Personal Information between Group Members. The purpose of this Privacy Training Requirements Protocol is to summarize how Group Members will train their staff, including employees, temporary, or part time employees, (collectively the "**employees**") on the requirements of the BCR Standards.

1.2 The Company's Legal & Compliance Department has overall responsibility for managing compliance training of Group Member employees. The Privacy training curriculum is overseen by the Company's **GCPO** and the Head of Privacy, the Global Privacy Network, and other regional and local Risk & Compliance and Legal professionals.

1.3 The training consists of multiple components including general training and both subject and country specific training, as well as BCR Standards training, all as described in Section 2 below, and all collectively referred to in this document as the "**Privacy Training Program.**"

2. DESCRIPTION OF THE COMPANY'S PRIVACY TRAINING PROGRAM

2.1 All Group Member employees worldwide, within 60 days of joining the Company, are required to complete training on *The Greater Good* – the Company's Code of Conduct ("**Code of Conduct**"). Subsequent training on the Code of Conduct is provided through an innovative video mini-series, entitled 'Choose Your Path' which dramatizes ethical dilemmas and tough issues that could arise in relation to seven key risk topics, including data protection. The training is designed to be both informative and user-friendly, generating interest in the topic; the individual modules are interactive, enabling employees to understand the impact of the choices they make.

2.2 Completion of the Choose Your Path training is monitored and enforced by the Group Members with oversight by the Company's Corporate Risk & Compliance team, which monitors the new-hire training and certification, recertification, and the 'Choose Your Path' training completion rates and reports them to the Audit Committee of the Company's Board of Directors.

2.3 Employees receive other training on a variety of compliance topics including information security and records management policies and procedures.

2.4 Group Members provide their employees with supplemental privacy training as needed, covering a range of subjects, including data privacy principles, the reporting and handling of data protection incidents, and handling subject access requests. Some of this privacy training focuses on particular country-law requirements such as those in Europe.

2.5 Employees who have permanent or regular access to European Personal Information including through collection, access, development of tools to process such European Personal Information, or any other processing activities, together with individuals in the internal audit team, (collectively "**EU Data Handlers**") shall receive additional, tailored training on the BCR Standards (the "**BCR Standards training**") and specific guidance relevant to their role. This training shall be repeated on a regular basis, as described below.

2.6 Employees receive a range of periodic communications such as emails, awareness messaging on intranet pages, and data privacy/information security posters displayed in offices all of which convey the importance of information security and data protection. Topics covered in such communications include: Protecting Personal Information, Clean Desk Standards, and Sending Information Securely.

3. AIMS OF THE COMPANY'S PRIVACY TRAINING PROGRAM

The aim of the Company's **Privacy Training Program** is to help create and maintain an environment in which:

(a) employees have an understanding of the basic principles of data privacy, confidentiality, and information security;

(b) employees understand the Company's privacy and information security policies and procedures; and

(c) EU Data Handlers receive appropriate training, as described in section 4, to enable them to process European Personal Information in accordance with the BCR Standards.

4. BCR STANDARDS TRAINING

4.1 The Company's training on the BCR Standards covers the following main areas:

(a) Background and rationale:

(i) What are the BCR Standards

(ii) How the BCR Standards work within the framework of European Data Protection Law

(b) The BCR Standards:

(i) The scope of the BCR Standards

(ii) Terminology and concepts

(iii) An explanation of how the BCR Standards work within the Company

(iv) The rights that the BCR Standards give to individuals

(v) The data protection and privacy implications arising from the processing of European Personal Information on behalf of Clients

(c) Where relevant to an employee's role, the BCR Standards training will also cover the following procedures:

(i) BCR Access Request Procedure

(ii) Audit Protocol

(iii) Updating Procedure

(iv) Co-operation Procedure

(v) Complaint Handling Protocol

5. FURTHER INFORMATION

Any queries about the BCR Standards training should be addressed to a member of the Global Privacy Network or sent via email to mmcbcr@mmc.com with the subject line: "BCR Training".

APPENDIX 4 - AUDIT PROTOCOL

1. BACKGROUND

1.1 The Company has adopted the BCR Standards to safeguard European Personal Information transferred between Group Members.

1.2 The BCR Standards require approval from Supervisory Authorities in the European Member States from which the European Personal Information is transferred. The Supervisory Authorities require the Company to audit its compliance with the BCR Standards and satisfy certain conditions in so doing. This document describes how the Company meets such requirements.

1.3 The role of the GCPO, the Head of Privacy and the Global Privacy Network whose roles and responsibilities are described in Appendix 2 of the BCR Standards is to provide guidance about the collection and use of European Personal Information subject to the BCR Standards and to assess the collection and use of such European Personal Information by Group Members for potential privacy-related risks. The collection and use of European Personal Information is, therefore, subject to detailed review and evaluation on an on-going basis. This Audit Protocol describes the formal assessment process adopted by the Company to assure compliance with the BCR Standards as required by the Supervisory Authorities, which operates alongside the work of the Global Privacy Network.

2. APPROACH

2.1 Overview of the BCR Standards audit programme

(a) Compliance with the BCR Standards is overseen on a day-to-day basis by the Global Privacy Network led by the GCPO.

(b) The Company's *Internal Audit Department*, which, operates across all of the Group Members, conducts its work in accordance with the Definition of Internal Auditing, the Code of Ethics, and the Standards for the Professional Practice of Internal Auditing as mandated by the Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF) and includes accredited auditors, will be responsible for performing and/or overseeing independent audits of compliance with the BCR Standards and will structure such audits to address all aspects of the BCR Standards. The *Internal Audit Department* will be responsible for verifying that any detected issues or instances of non-compliance are also brought to the attention of the Head of Privacy, appropriate member of the Global Privacy Network, or the GCPO (in accordance with section 2.4 below), and that any corrective actions to drive compliance take place within a reasonable timeframe.

(c) To the extent that the Company acts as a processor, audits of compliance with the commitments made in the Processor Standard may also be

carried out by or on behalf of the Company's Clients in accordance with the terms of a contract the Company has with a Client in respect of such processing. Such audits may also extend to any sub-processors acting on the Company's behalf in respect of such processing and the ability to audit such sub-processors will be carried out in accordance with the terms of the contract between the Company and the sub-processors.

2.2 **Timing and scope of audit**

(a) Audit of the BCR Standards will take place:

(i) annually in accordance with the internal audit department's audit procedures and controls; and/or

(ii) more frequently at the request of the GCPO; and/or

(iii) as determined necessary by members of the Global Privacy Network.

(b) To the extent that a Group Member processes European Personal Information on behalf of a Client, audit of compliance with the Processor Standard will take place in accordance with the contract in place between that Group Member and that Client.

(c) The scope of any audit performed pursuant to this audit protocol will be determined by the audit team applying a risk-based approach that will consider relevant criteria, such as: areas of known non-compliance; areas of current regulatory focus; areas of specific or new risk for the business; reported areas of concern; areas with changes to the systems or processes used to safeguard European Personal Information; areas where there have been previous audit findings or complaints; the period since the last review; and the nature, method and location of the European Personal Information processed.

(d) In the event that a Client on whose behalf the Company processes European Personal Information exercises its right to audit the Company for compliance with the Processor Standard, the scope of the audit shall be limited to the data processing facilities, data files and documentation relating to that Client's data, all in accordance with the terms of a contract the Company has with the Client in respect of such processing. The Company will not provide a Client with access to systems which do not process European Personal Information of that Client or arrange audits in such a way as to compromise the personal information of other clients.

2.3 **Auditors**

(a) Audit of the procedures and controls in place to give effect to the commitments made in the BCR Standards will be undertaken by;

(i) Members of Internal Audit; and/or

(ii) other accredited internal/external auditors/examiners as determined by the VP of Internal Audit as necessary to assist one of the above parties.

(b) In the event that a Client on whose behalf the Company processes European Personal Information exercises its right to audit the Company for compliance with the Processor Standard, such audit may be undertaken by that Client or by independent, accredited auditors selected by that Client to the extent provided in the contract between the Company and that Client.

2.4 **Report**

(a) On completion of the audit, the report and findings will be made available to the Head of Privacy, GCPO and the relevant member(s) of the Global Privacy Network. A summary of the findings will be shared with senior management according to pre-existing distribution lists and further disseminated to the appropriate impacted parties with details of any remedial action required, recommendations and timescales for remedial action to be undertaken. Internal Audit will also provide report results of audit activity to the audit committee of the Company board of directors.

(b) Upon request, the Company has agreed to:

(i) provide copies of the results of any audit of the BCR Standards to a competent Supervisory Authority and in accordance with their applicable audit procedures who will, upon receiving the audit results, be reminded of their duties of professional secrecy under Article 54(2) of the GDPR; and

(ii) to the extent that an audit relates to European Personal Information processed by the Company on behalf of a Client, to make the results of any audit of compliance with the Processor Standard available to that Client, in accordance with the terms of a contract the Company has with such Client and taking into account the Company's right to protect certain types of information, including business sensitive data or trade secrets.

(c) The Company's GCPO and/or the relevant member(s) of the Global Privacy Network will be responsible for liaising with the Supervisory Authorities for the purpose of providing the information outlined in section 2.4(b).

(d) In addition, the Company has agreed that Supervisory Authorities may audit Group Members for the purpose of reviewing compliance with the BCR Standards in accordance with their applicable audit procedures.

APPENDIX 5A - COMPLAINT HANDLING PROTOCOL – EXTERNAL

1. BACKGROUND

1.1 The Company has adopted the BCR Standards to safeguard European Personal Information transferred between Group Members.

1.2 The BCR Standards require approval from Supervisory Authorities in the European Member States from which the European Personal Information is transferred. The Supervisory Authorities require the Company to maintain a process to address complaints from individuals whose European Personal Information is processed under the BCR Standards. This document describes how the Company meets such requirements.

2. APPROACH

2.1 The Company is committed to handling complaints raised by individuals in a fair and professional manner.

2.2 Affected individuals (such as clients, suppliers, other third parties, or employees of such entities) may raise a complaint if their European Personal Information is processed by the Company and such processing falls within the scope of the BCR Standards.

2.3 Individuals have various options for raising a complaint. All complaints must be made in writing.[1] Unless a pre-existing complaint channel has been communicated to an individual through his or her employer or the Company in which case the individual should send the complaint via the pre-existing complaint channel, the individual may send a complaint to any of the following (each, a "**Complaint Handler**"):

(a) to the Company manager responsible for the relationship with the supplier, client or third party pursuant to which the European Personal Information was processed;

(b) to the Head of Privacy at mmcbcr@mmc.com preferably with the subject line: "BCR Complaint";

(c) in writing to: Marsh & McLennan Ireland Limited, (FAO: Head of Privacy), Marsh House, 25-28 Adelaide Road, Dublin 2;

(d) to the Company's Ethics & Compliance Line, a free, secure and confidential resource, accessible online or by telephone 24 hours a day, 7 days a week, worldwide. Detailed instructions for access can be found here: www.EthicsComplianceLine.com; or

[1] Unless the local data protection law permits a complaint to be made orally, in which case the Company will document the complaint and provide a copy to the individual making the complaint before dealing with it in accordance with this Protocol.

(e) if the matter relates to European Personal Information that has been exported outside Europe, to the Group Member responsible for exporting such European Personal Information.

2.4 In cases where the Company acts as a Processor for the information subject to a complaint, or a complaint relates to the Processor Standard, the Company will, without undue delay, refer the complaint to the Client for handling, unless:

(a) the terms of the contract between the Company and the Client require (or allow) for the handling of such complaints by the Company; or

(b) the Client has disappeared, no longer exists or has become insolvent;

in those cases the Company will deal with such complaints in accordance with this Complaint Handling Protocol.

2.5 Once a complaint is received by a Complaint Handler, he or she will liaise with the relevant business or functional team to investigate the complaint. The Complaint Handler will acknowledge receipt of the complaint within five (5) working days, and it shall ordinarily investigate and issue a substantive response to the complainant within one month of the date the complaint was received. If, due to the complexity or number of the complaint(s), a substantive response cannot be given within this period, the Complaint Handler will advise the complainant of the reason for the delay within one month of receipt of the complaint and give a reasonable estimate for the timeframe within which a response and resolution to the complaint will be provided and in any event will resolve the complaint within two (2) months of the date on which the individual was notified of the extension.

2.6 Complaint Handlers shall also forward a copy of the complaint and any communications with the complainant to a member of the Global Privacy Network so that the complaint can be logged in a central database for tracking and reporting purposes.

2.7 If the complaint is upheld, the Complaint Handler (or the Group Member or function responsible for the processing relevant to the complaint) will arrange for any necessary corrective steps to be taken as a consequence of the complaint.

2.8 If the complainant is not satisfied with the initial response or any aspect of the handling of his or her complaint, the Complaint Handler will provide the contact details of the GCPO (or, in those cases where the matter was handled in the first instance by the GCPO, to the Company's Deputy Chief Compliance Officer), so that the complainant may ask them to review the initial decision. The GCPO (or Deputy Chief Compliance Officer) will review the case and advise the complainant of his/her decision either to accept the original finding or to substitute a new finding. The GCPO (or Deputy Chief Compliance Officer) will respond to the complainant within one (1) month of the referral or may extend that period by two (2) further months where necessary taking into consideration

the complexity and number of the requests, informing the complainant of the reasons for the delay.

2.9 If the complaint is upheld, the GCPO/Deputy Chief Compliance Officer (or the Group Member or function responsible for the processing relevant to the complaint) will arrange for any necessary corrective steps to be taken as a consequence of the complaint.

2.10 Complainants also have the right to:

(a) complain to a competent Supervisory Authority in the jurisdiction in which the alleged infringement took place, or in which the individual works or habitually resides; and/or

(b) lodge a claim with a court of competent jurisdiction, as described in Section C of the relevant BCR Standard.

These rights apply whether or not the complainant has first made a complaint to the Company.

APPENDIX 5B

Privacy Complaints Handling Protocol - Internal

MARSH & MCLENNAN COMPANIES

BCR - COMPLAINTS HANDLING PROTOCOL (INTERNAL)

Issued: January 2023

COMPLAINTS HANDLING PROTOCOL (INTERNAL)

SUMMARY

Marsh & McLennan Companies, Inc. and certain of its businesses (collectively the "Company") has obtained approval from European regulators for a special framework to allow the Company to transfer personal information which is subject to European[1] data protection law ("European Personal Information") to any entity outside Europe that is part of the Company and participates in the framework. This framework is known as Binding Corporate Rules ("BCR"). Under the BCR, the Company has agreed to make available to all colleagues whose European Personal Information is processed under the BCR a special procedure to complain about the handling of their European Personal Information (hereinafter, a "Privacy Complaint") by the Company.

SCOPE

This protocol applies to complaints of Company officers, employees and temporary employees ("colleagues") with respect to the manner in which their European Personal Information is collected, used, disclosed, transferred, retained, or destroyed by the Company (collectively referred to as "processing") insofar as such processing is covered by the BCR. In other words, a Privacy Complaint is an expression of dissatisfaction specifically related to the Company's compliance with its BCR when it comes to the processing of colleague European Personal Information.

All other colleague complaints should be handled in the ordinary course under other existing Company policies and procedures.

There is a separate complaint handling protocol for handling complaints of clients, suppliers and other third parties relating to the processing of their European Personal Information under the BCR.

DATA HANDLING OBLIGATIONS

The Company's obligations with respect to the processing of colleague European Personal Information are set forth in the BCR.

PRIVACY COMPLAINT HANDLING APPROACH

General

The Company is committed to promptly and appropriately investigating the allegations of each Privacy Complaint submitted to it.

Complaint Submission

Privacy Complaints must be submitted in writing[2] to the Head of Privacy at mmcbcr@mmc.com or in writing to Marsh & McLennan Ireland Limited (FAO: Head of Privacy), Marsh House, 25-28 Adelaide Road, Dublin 2 preferably with the subject line: "BCR

1 References to Europe for the purposes of this document mean the EEA and Switzerland.

2 Unless the local data protection law permits a complaint to be made orally, in which case the Company will document the complaint and provide a copy to the individual making the complaint before dealing with it in accordance with this Protocol.

Complaint," and specifying the European Personal Information impacted, the processing activity being complained about, and any other pertinent details. Once received, the complaint will be referred to a Complaint Handler, as described below.

Complaint handling

Each business shall designate one or more individuals as Complaint Handlers. The Head of Privacy is responsible for oversight of the Complaint Handlers. Once a complaint is received by a Complaint Handler, he or she may liaise with the relevant business or functional team to investigate the complaint and to institute remedial action.

The Company will acknowledge the complaint within five (5) business days and aim to provide a complete response within one month. If the complaint cannot be resolved within this timeframe because it requires a more detailed investigation, the Company will contact the complainant and provide an update, including the reason for the delay (for example, due to the complexity of the request or the number of requests), within one month of receipt of the complaint, and give a reasonable estimate of the timeframe within which the response will be provided. The Company will resolve the complaint within two (2) months of the date on which the individual was notified of the extension. If the complaint is upheld, the Complaint Handler will arrange for any necessary corrective steps to be taken as a consequence.

Further rights

If the complainant is not satisfied with the initial response or any aspect of the handling of his or her complaint, the Complaint Handler will provide the contact details of the GCPO (or, in those cases where the matter was handled in the first instance by the GCPO, the Company's Deputy Chief Compliance Officer), so that the complainant may ask them to review the initial decision. The GCPO (or Deputy Chief Compliance Officer) will review the case and advise the complainant of his/her decision either to accept the original finding or to substitute a new finding. The GCPO (or Deputy Chief Compliance Officer) will respond to the complainant within one (1) month of the referral or may extend that period by two (2) further months where necessary taking into consideration the complexity and number of the requests, informing the complainant of the reasons for the delay. The GCPO (or Deputy Chief Compliance Officer) will be responsible for initiating any necessary remedial action.

Colleagues based in Europe whose European Personal Information is processed under the BCR also have the right to: i) complain to a competent Supervisory Authority in the jurisdiction in which the alleged infringement took place, or in which the individual works or habitually resides; and/or ii) lodge a claim with a court of competent jurisdiction, as described in the BCR. This right applies whether or not the complainant has first made a complaint to the Company.

Complaints related to handling of European Personal Information by third parties

To the extent that the Privacy Complaint relates to colleague European Personal Information that was being processed by a third party on behalf of the Company, the Complaint Handler will raise the matter with the relevant third party, working through the relevant sourcing and procurement or HR channels where applicable.

APPENDIX 6 - CO-OPERATION PROCEDURE

1. INTRODUCTION

This Co-operation Procedure sets out the way in which the Company will co-operate with the Supervisory Authorities in relation to the BCR Standards.

2. CO-OPERATION PROCEDURE

2.1 Where required, the Company will make the necessary personnel available for dialogue with a Supervisory Authority in relation to the BCR Standards.

2.2 The Company will actively review and consider:

(a) any decisions made by competent Supervisory Authorities on any European Data Protection Law issues that may affect the BCR Standards; and

(b) the views of the European Data Protection Board and any successor body as outlined in its published guidance on Binding Corporate Rules for controllers and Binding Corporate Rules for processors.

2.3 The Company will provide upon request copies of the results of any audit of the BCR Standards to a Supervisory Authority of competent jurisdiction and in accordance with their applicable audit procedures who will, upon receiving the audit results, be reminded of their duties of professional secrecy under Article 54(2) of the GDPR.

2.4 The Company agrees that:

(a) where any Group Member is located within the jurisdiction of a Supervisory Authority, that particular Supervisory Authority may audit that Group Member for the purpose of reviewing compliance with the BCR Standards; and

(b) in the case of a Group Member located outside of Europe, a Supervisory Authority may audit that Group Member for the purpose of reviewing compliance with the BCR Standards in accordance with the applicable law of the European country from which the European Personal Information is transferred under the BCR Standards (which, when the Company acts as a processor on behalf of a third party controller, will be determined by the place of establishment of the controller).

2.5 Such audit may be carried out by a Supervisory Authority of competent jurisdiction and in accordance with their applicable audit procedures who will, when carrying out the audit, be reminded of their duties of professional secrecy under Article 54(2) of the GDPR.

2.6 Without prejudice to the right to appeal, the Company agrees to abide by the advice of the applicable Supervisory Authority.

APPENDIX 7 - UPDATING PROCEDURE

1. INTRODUCTION

This Binding Corporate Rules Updating Procedure sets out the way in which the Company will communicate changes to the BCR Standards to the Supervisory Authorities, data subjects, its Clients and to Group Members bound by the BCR Standards.

2. MATERIAL CHANGES TO THE BCR STANDARDS

2.1 The Company will communicate any material changes to the BCR Standards to the Irish Data Protection Commission ("**Irish DPC**") without undue delay, and via the Irish DPC, to any other competent Supervisory Authorities.

2.2 Where a change to the Processor Standard affects the conditions under which the Company processes European Personal Information on behalf of any Client under the terms of its contract with the Company, the Company will also communicate such information to the affected Client before it is implemented, with sufficient notice to enable the affected Client to object. The Client may also seek to suspend the transfer of European Personal Information to the Company and/or terminate the contract, all in accordance with the terms of its contract with the Company.

3. ADMINISTRATIVE CHANGES TO THE BCR STANDARDS

3.1 The Company will communicate changes to the BCR Standards which are administrative in nature (including changes in the list of Group Members) or which have occurred as a result of a change of European Data Protection Law, through any legislative, court or Supervisory Authority measure, to the Irish DPC and to any other relevant Supervisory Authorities at least once a year. The Company will also provide a brief explanation to the Irish DPC (and any other competent Supervisory Authorities) of the reasons for any changes to the BCR Standards.

3.2 The Company will make available changes to the Processor Standard which are administrative in nature (including changes in the list of Group Members) or which have occurred as a result of a change of European Data Protection Law, through any legislative, court or Supervisory Authority measure, to any Client on whose behalf the Company processes European Personal Information.

4. COMMUNICATING AND LOGGING CHANGES TO THE BCR STANDARDS

4.1 The BCR Standards contain a change log which sets out the date of revisions to the BCR Standards and the details of any revisions made.

4.2 The Head of Privacy with the support of the Regional Privacy Teams will communicate all changes to the BCR Standards, whether administrative or material in nature:

(a) to the Group Members bound by the BCR Standards through its internal communication channels; and

(b) to Clients on whose behalf the Company processes European Personal Information and to the data subjects who benefit from the BCR Standards via the Company website (https://www.marshmclennan.com/privacy-statement.html) and any other channels it uses to communicate with Clients.

4.3 The Head of Privacy will maintain an up to date list of the changes made to the BCR Standards and the list of Group Members bound by the BCR Standards. This information may be requested by submitting an email to mmcbcr@mmc.com with the subject line: "BCR Changes".

4.4 For the purposes of the Processor Standard, the Company shall maintain a list of the Sub-Processors appointed by the Company to process European Personal Information on behalf of its Clients through it sourcing and operations teams which will be made available on request in relation to the processing carried out on behalf of the requester.

5. NEW GROUP MEMBERS

The Company's Global Chief Privacy Officer together with the network of privacy leaders and privacy coordinators in the various Group Members' countries will assure that all new Group Members accede to the Intra-Group Agreement and are bound by the BCR Standards and can deliver compliance before a transfer of European Personal Information to them takes place under the BCR Standards.

APPENDIX 8 – PROCESSING SCHEDULE

The Controller (as defined in Part 1 to this Processing Schedule ("**Part 1**")) wishes to appoint the Processor (also as defined in Part 1) to process certain European Personal Information on its behalf in accordance with Rule 4D. The Controller and the Processor have elected to complete this Processing Schedule as the means by which to satisfy the requirements of the GDPR.

This Processing Schedule is to be read and interpreted in conjunction with the Controller Standard.

Part 1: Processing Instructions

1.1. Name of Group Member as controller: ……..……(the "**Controller**")

1.2 Name of Group Member as processor: ……..……(the "**Processor**")

1.3 Purpose of the processing carried out by the Processor: …….....

1.4 The European Personal Information processed will include the following categories of personal information:

(a) [*list each category of personal information which will be processed, e.g. names, email addresses, financial information*]

1.5. The data subjects to whom the personal information relates are:

(a) [*list each category of data subjects, e.g. clients*]

1.6. The activities to be carried out by the Processor on behalf of the Controller will consist of:

(a) [*describe services carried out by the Processor on the Controller's behalf in detail*]

1.7. Duration of processing carried out by the Processor: …….....

Part 2: Processor's Obligations

2. The Processor shall:

2.1 ensure that personnel/contractors authorised to process the European Personal Information described in Part 1 (the "**Data**") have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

2.2 inform the Controller: i) if it is legally required to process the Data otherwise than as instructed by the Controller before such processing occurs, unless the law requiring such processing prohibits the Processor from notifying the Controller,

in which case it will notify the Controller as soon as that law permits it to do so; and ii) about any instruction from the Controller which, in the Processor's opinion, infringes applicable data protection law;

2.3 not subcontract any processing of the Data or otherwise disclose the Data to any third party except as authorised by the Controller in writing. Where sub-contracting is permitted the Processor will: (a) ensure that it has a written contract (the "**Processing Subcontract**") in place with the relevant subcontractor which imposes on the subcontractor the same obligations in respect of processing of the Data as are imposed on the Processor under Rule 4D and this Part 2 to the Processing Schedule ("**Part 2**"); (b) ensure that there are sufficient guarantees in place to ensure the Processing Subcontract meets the requirements of Article 28 of the GDPR; (c) remain fully liable to the Controller for its obligations under Rule 4D and this Part 2; and (d) ensure that Rule 6 of the Controller Standard is complied with in the event that Data is subject to a trans-border transfer to a sub-contractor;

2.4 upon completion of the processing carried out by the Processor on the Controller's behalf and at the choice of the Controller, return or delete all Data processed by the Processor and all copies of such information unless the Processor is prevented from doing so by European or Member State law to which the Processor is subject, in which case the Data will be kept confidential and will not be actively processed for any purpose; and

2.5 provide such information, co-operation and assistance as the Controller reasonably considers to be necessary to enable the Controller to: (a) verify Processor's compliance with Rules 4A and 4D of the Controller Standard and this Processing Schedule, including allowing for and contributing to audits and inspections by the Controller or another auditor mandated by the Controller; (b) carry out prior assessments of processing activities which are likely to result in a high risk to the rights and freedoms of individuals and any related consultations with competent Supervisory Authorities; (c) fulfil its obligations in respect of any request by an individual to exercise their rights under the Controller Standard, including by notifying the Controller without undue delay of any such request; and (d) investigate, mitigate and notify in accordance with Rule 4B of the Controller Standard any Data Protection Breach involving the Data, including by notifying the Controller without undue delay of any such Data Protection Breach.