DATED 2023

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

CONTENTS

INTRODUCTION

This Processor Standard establishes the approach of the Company to the protection and management of European Personal Information globally by Group Members.

Group Members and employees must comply with and respect this Processor Standard when processing personal information as data processors.

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

"**Client**" means the Third Party client (as Controller) which is subject to European Data Protection Law.

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

References to a "**contract**" in this Processor Standard are to a contract which meets the requirements of applicable European Data Protection Law.

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

"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 Europe, 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.

"**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.

"**Individual**" means an identified or identifiable natural person.

"**Personal Information**" means any information relating to an **Individual**.

"**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.

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

"**Sub-Processor**" means a third party engaged by or on behalf of a Processor that will Process Personal Information as part of the performance of the Services (including Third Country Recipients).

"**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.

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

Information about this Processor 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.

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. 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 requirements.

When, on the other hand, a company processes personal information on behalf of a Third Party, it is deemed to be a *processor* of the information and the third party will be primarily responsible for meeting the legal requirements. So, for example, where a company provides services as a global benefits outsourcing provider to a Client, it will be acting as a processor in respect of the personal information of the Client who is the controller.

1.2 How does data protection law affect the Company internationally?

European Data Protection Laws do not allow the transfer of Personal Information to countries outside 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.

When a Group Member acts as a Processor and/or Sub-Processor, the Group Member's Client also retains its responsibility to comply with European Data Protection Laws.

In practical terms, this means that those Clients must pass certain data protection obligations onto any Processor that Processes Personal Information outside Europe on their behalf. By imposing those obligations on the Processor, the Client satisfies the legal restrictions on international data transfers.

In the event that a Group Member fails to comply with the data protection obligations imposed on it by its Clients, it may cause the Clients to be in breach of applicable data protection law and the Group Member may then face a claim for breach of contract. That claim may result in the payment of compensation or other judicial remedies. In such cases, if a Client can demonstrate that it is likely that the damage has occurred because of a breach of this Processor Standard, the burden of proof to show that a non-European Group Member (or any Third Party Sub-Processor which is established outside Europe and which is acting on behalf of a Group Member) is not responsible for the breach, or that no such breach took place, will rest with the European Group Member transferring the

European Personal Information to the Group Member outside Europe. In addition, a Client that has entered into a contract with a Group Member that incorporates this Processor Standard may enforce this Processor Standard in the European courts, where permitted by law and subject to the terms of the contract with the Client, against: (i) any Group Member processing European Personal Information on behalf of that Client in respect of a breach of the Processor Standard caused by that Group Member or any Sub-Processor established outside of the EU; and (ii) the Group Member that exported such Personal Information to the Group Member in (i).

1.3 **What is the Company doing about it?**

The Company takes privacy seriously. The purpose of this Processor Standard is to set out a framework to satisfy the standards contained in European Data Protection Law. Processes required by this Standard provide a level of protection that is equivalent to that which is guaranteed under European Data Protection Law for European Personal Information transferred to Group Members outside Europe.

Group Members will apply the Rules contained in this Processor Standard whenever they Process European Personal Information as a Processor or a Sub-Processor in the course of providing services to a Client, absent a separate arrangement in such Client contract. Where the Company's Client wishes to rely upon this Processor Standard as providing adequate safeguards, a copy of this Processor Standard shall be incorporated into the contract with that Client. If a Client chooses not to rely upon this Processor Standard, and opts to follow the contract already in place with the Company (or other terms), each party will comply with its responsibility to put in place any other safeguards necessary to protect the European Personal Information in accordance with European Data Protection Law.

This Processor Standard applies to all Group Members and their employees worldwide and requires that Group Members that Process European Personal Information as a Processor or a Sub-Processor in the course of providing services to a Client comply with the Rules set out in clause 2 of this Processor Standard together with the policies and procedures set out in the appendices listed in clause 3 of this Processor Standard.

Group Members must comply with the Binding Corporate Rules Controller Standard when they Process European Personal Information as a Controller. Some Group Members may act as a Controller (or a Controller and a Processor to another Group Member) *and* a Processor to a Client and must therefore comply with this Processor Standard and also the Binding Corporate Rules Controller Standard as appropriate.

1.4 **What personal information does this Processor Standard cover?**

European Personal Information Processed under this Processor Standard is transferred to allow the Group Member acting as a Processor to provide services to Clients, and falls within the following categories:

- Personal Information relating to a Group Member's Clients and employees of such Clients. In particular, this Personal Information includes family names, given names, titles, employer and job title, e-mail address, phone number; and/or
- Personal Information relating to customers of a Group Member's Clients and other third parties to the extent that access to such Personal Information is required in order for the Group Member to provide these services. This Personal Information includes family names, given names, titles, employer and job title, information relating to the service provided (for example, retirement dates, benefits provision).

This Personal Information is Processed in order to enable the Company to provide Clients with:

- risk and insurance services, including risk management services (risk advice, risk transfer, and risk control and mitigation solutions), and insurance and reinsurance broking and services; and
- consulting services, including health, retirement, pension administration, talent and investments services and products, and specialised management and economic consulting services.

Transfers of European Personal Information may take place from Group Members in Europe to any of the Group Members located outside Europe.

1.5 **Further information**

Questions regarding the provisions of this Processor Standard, Individuals' rights arising under this Processor 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 Processor 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, he or she may bring the matter to the Company's attention by using the complaint handling procedures which are set out in Appendix 5.

2. PROCESSOR OBLIGATIONS

Clause 2 of this Processor Standard is divided into three sections:

- **Section A** addresses the basic principles that a Group Member must observe when it Processes European Personal Information as a Processor or a Sub-Processor in the course of providing services to a Client.
- **Section B** summarises the practical commitments made by Group Members to the Supervisory Authorities when Group Members Process European Personal Information as a Processor or a Sub-Processor in the course of providing services to a Client.
- **Section C** describes the third party beneficiary rights that the Group Members have granted to Individuals in its capacity as a Processor or a Sub–processor under this Processor Standard.

SECTION A: BASIC PRINCIPLES

RULE 1 – COMPLIANCE WITH LOCAL LAW

Rule 1A – the Company will assure that compliance with this Processor Standard will not conflict with data protection laws where they exist.

Group Members 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 Processor Standard applies and applicable data protection legislation requires a higher level of protection than is provided for in this Processor Standard, the Company acknowledges that it will take precedence over this Processor Standard.

Rule 1B – the Company will co-operate and assist a Client to comply with its obligations under European Data Protection Law in a reasonable time and to the extent reasonably possible.

Group Members will, taking into account the nature of Processing and information available to the Group Member, within a reasonable time and to the extent reasonably possible and as may be required under contracts with their Clients, assist the Clients with requests to comply with their obligations as Controllers under applicable European Data Protection Law. For example, Group Members will be transparent about Sub-Processor activities so that their Clients may correctly inform the relevant Individuals.

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

Rule 2A – the Company will assist a Client to comply with the requirement to explain to Individuals at the time their European Personal Information is collected how that information will be Processed.

The Clients of Group Members have a duty to explain to Individuals, at the time their European Personal Information is collected, how that information will be Processed. Group Members will provide such assistance and information to their Clients as may be required under the terms of the contracts with their Clients to comply with this requirement. This includes, for example, providing information about any Sub-Processors appointed by a Group Member to Process European Personal Information on a Client's behalf.

Rule 2B – the Company will only Process European Personal Information on behalf of and in accordance with the instructions of the Client.

Group Members and their employees will only Process European Personal Information in compliance with the terms of the contracts they have with their Clients, including in relation to transfers of European Personal Information to destinations outside Europe.

Group Members will immediately inform the Client if, in their opinion, an instruction infringes European Data Protection Law.

If, for any other reason, a Group Member is unable to comply with this Rule or its obligations under this Processor Standard in respect of any contract it may have with a Client, the Group Member will inform the Client promptly of this fact and further will inform the Client of any additional legal requirement as required by Union or Member State law to which the Group Member is subject. The Group Member's Client may then suspend the transfer of European Personal Information to the Group Member and/or terminate the contract, depending upon the terms of its contract with the Group Member.

On termination of a Group Member's contract with a client, the Group Member will act in accordance with the contract and any instructions of its Client in the return or destruction of the European Personal Information and, where required by Client contract, the certification of such, including any copies of such information, in a secure manner or as otherwise required by its Client.

In the event that Member State law prevents the Group Member from returning the Personal Information to its Client or destroying it, the Group Member will assure that such information remains confidential and will not Process the Personal Information otherwise than in accordance with the instructions of the Client or as required by applicable law.

RULE 3 – DATA QUALITY AND PROPORTIONALITY

Rule 3 – the Company will cooperate with Clients' actions to keep European Personal Information accurate and up to date.

Group Members will modify their databases and systems to reflect updates or anonymization of or deletions to European Personal Information when provided by Clients.

Where a Client requests deletion or anonymization of European Personal Information and that Personal Information cannot, for technical, legal or regulatory reasons, be deleted, the Group Member will advise the Client accordingly and shall assure that such Personal Information is not used in the provision of services.

A Group Member will notify other Group Members or any Third Party Sub-Processor to whom the Personal Information has been disclosed of any rectification or deletion or anonymization so that they can also update their records.

RULE 4 – RESPECTING INDIVIDUALS' RIGHTS

Rule 4 – the Company will assist Clients to comply with the rights of Individuals.

Taking into account the nature of the Processing, Group Members will act in accordance with the instructions of their Clients and undertake any reasonably necessary measures, and will execute any appropriate technical and organizational measures, to enable their Clients to comply with their duty to respect the rights of Individuals. In particular, if any Group Member receives a request, the Group Member will transfer such request promptly to the relevant Client and not respond to such a request unless authorised to do so. Group Members will follow the steps set out in section 7 of the BCR Individuals' Rights Request Procedure (see Appendix 1).

RULE 5 – SECURITY AND CONFIDENTIALITY

Rule 5A – the Company will implement the appropriate technical and organisational security measures and as specified in a contract with a Client.

Where a Group Member provides a service to a Client that involves the Processing of European Personal Information, the contract between that Group Member and its Client needs to impose clear and specific obligations on the processor dealing with the security of that information and which meet the requirements of applicable European Data Protection Law. This is in order to assure that the Group Member has in place appropriate technical and organisational security measures to ensure a level of security to the Personal Information appropriate to the risk presented by the Processing.

Group Members will adhere to the security and organisational measures specified in contracts with their Clients and will assist Clients in implementing appropriate technical and organisational measures to facilitate compliance with this Processor Standard in practice (such as data protection by design and by default) so far as is reasonable taking into account the state of the art, cost of implementation, risks to Individuals, and nature, scope, context and purpose of the Processing.

Rule 5B – the Company will notify a Client of any security breach in accordance with the terms of the contract with that Client.

Group Members will notify Clients of any 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**") on behalf of those Clients without undue delay and in accordance with the terms of the Group Member's contract with the Clients. If Sub-Processors are appointed in accordance with Rule 5C below, Sub-Processors will inform the Client and the processor Group Member of any such Data Protection Breach without undue delay.

Rule 5C – the Company will comply with the requirements of a Client regarding the appointment of any Sub-Processor.

Group Members will inform their Clients where processing of European Personal Information on their behalf will be conducted by an internal or external Sub-Processor, and will comply with the particular requirements of a Client with regard to the appointment of Sub-Processors as set out under the terms of its contract with that Client and in particular will obtain prior informed specific or general written authorisation of the Client regarding the appointment of any Sub-Processors. Where the Client has provided general written authorisation, Group Members will assure that up to date information regarding the appointment of Sub-Processors is available to its Clients so that their general consent to Sub-processing is obtained before the data have been transferred to a new Sub-Processor. If, on reviewing this information, a Client objects to the appointment of a Sub-Processor to Process European Personal Information on its behalf, that Client will be entitled to take such steps as are consistent with the terms of its contract with a Group Member and as referred to in Rule 2B of this Processor Standard.

Rule 5D – the Company will assure that Sub-Processors undertake to comply with provisions which are consistent with (i) the terms in its contracts with its Clients and (ii) this Processor Standard, and in particular that the Sub-Processor will adopt appropriate and equivalent security measures.

Group Members shall only appoint Sub-Processors who provide sufficient guarantees in respect of the commitments made by Group Members in this Processor Standard. In particular, such Sub-Processors must be able to provide appropriate technical and organisational measures that will govern their

Processing of the European Personal Information to which they will have access in accordance with the terms of the Group Member's contract with its Clients.

To comply with this Rule, where a Sub-Processor has access to European Personal Information, the Group Member will take steps to assure that it has in place appropriate technical and organisational security measures to safeguard that Personal Information and will impose strict contractual obligations in writing on the Sub-Processor which provide:

- commitments on the part of the Sub-Processor regarding assistance in compliance with this Processor Standard, data quality, transparency and purpose limitation principles, Individuals' rights and security of that information consistent with those contained in this Processor Standard (and in particular Rules 1, 2, 3, 4, 5A and 5B above) and with the terms of the contract the Group Member has with its Clients in respect of the Processing in question;

- that the Sub-Processor will act only on the Group Member's instructions when Processing European Personal Information;

- adequate safeguards (as understood in European Data Protection Law) with respect to the transfer of European Personal Information from a Group Member in Europe to a Sub-Processor established in a non-adequate jurisdiction; and

- such obligations as may be necessary to ensure that the commitments on the part of the Sub-Processor reflect those made by the Group Member in this Processor Standard.

SECTION B: PRACTICAL COMMITMENTS

RULE 6 – COMPLIANCE AND ACCOUNTABILITY

Rule 6A – the Company will have appropriate resources to oversee compliance with this Processor Standard throughout the Group Members.

The Company has appointed its GCPO as the person to oversee compliance with this Processor 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 Processor 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 6B – 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;
- the name and contact details of each Client on whose behalf the Group Member processes European Personal Information and, where applicable, of the Client's representative and data protection officer;
- the categories of Processing carried out on behalf of each Client;
- details of the third country or countries to which European 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; and
- where possible, a general description of the technical and organisational security measures used to protect European Personal Information.

RULE 7 – TRAINING

Rule 7 – the Company will provide appropriate training to employees who have permanent or regular access to European Personal Information, who are involved in the collection of European Personal Information or in the development of tools used to process European Personal Information in accordance with the Privacy Training Requirements Protocol attached as Appendix 3.

RULE 8 – AUDIT

Rule 8 – the Company will comply with the Audit Protocol set out in Appendix 4.

RULE 9 – COMPLAINTS

Rule 9 – 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 10 – CO-OPERATION WITH SUPERVISORY AUTHORITIES

Rule 10 – the Company will comply with the Co-operation Procedure set out in Appendix 6.

RULE 11 – UPDATES TO THE PROCESSOR STANDARD

Rule 11 – the Company will comply with the Updating Procedure set out in Appendix 7.

RULE 12 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE PROCESSOR STANDARD

Rule 12A – the Company will carry out a transfer impact assessment before making transfers under this Processor Standard.

The Company will carry out a transfer impact assessment to assess if the legislation applicable to Non-European Group Members prevents them from fulfilling their obligations under this Processor Standard or has a substantial effect on the guarantees provided under this Processor Standard before making transfers of European Personal Information under this Processor 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 Processor 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 Processor 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 this Processor 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 European Group Member, destroyed or returned to the European Group Member. In any event, the European Group Member can choose to end the transfer following such suspension.

If a Group Member decides to continue the transfer after identifying that no additional safeguards could be put in place, the Client will be entitled to suspend the transfer of European Personal Information and/or terminate the contract with the Company, as provided for in Rule 2B.

Rule 12B – the Company will ensure that where a Group Member believes that the legislation applicable to it prevents it from fulfilling the instructions received from the Client, its obligations under this Processor Standard or its contract with the Client, such Group Member will promptly inform (unless otherwise prohibited by law):

- **the Client, as provided for in Rule 2B;**
- **the GCPO and/or the MMC Head of Privacy, EMEA ("Head of Privacy"); and**
- **the Supervisory Authority competent for the Client and the Group Member.**

In addition to the above:

- Non-European Group Members will notify European Group Members where there is a change in the laws of the third country which could affect the results of the initial transfer impact assessment carried in accordance with Rule 12A; and
- European Group Members 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 12A.
- Upon verification of such notification, European Group Members, 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 European Group Member and/or the Non-European Group Member in order to enable them to fulfil their obligations under this Processor Standard. The same applies if a European Group Member has reason to believe that a Non-European Group Member can no longer fulfil its obligations under this Processor Standard.
- Where the European Group Member (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 12C – the Company will ensure that where a Group Member 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 Processor Standard, the relevant Group Member will, unless prohibited from doing so:

- **promptly notify the Client; and**
- **put the request on hold and promptly notify the Supervisory Authority competent for the Client and the Processor.**

Where a Group Member receives a legally binding request for disclosure of European Personal Information from a law enforcement authority or a state security body and is prohibited from putting the request on hold and/or from notifying the competent Supervisory Authorities, the Group Member 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 Processor Standard.

In these cases, 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. Where European Personal Information is transferred under this Processor Standard by a European Group Member pursuant to a contract with a Client, the Individual to whom that European Personal Information relates will have the right as a third party beneficiary to enforce Rules 1B, 2, 3, 4, 5, 9, 10, and 12, the right to easy access to information to which such Individuals are entitled regarding this Processor Standard and the right to enforce the provisions in this Section C(2),(4),(5),(6),(7),(8),(9), granting third-party beneficiary rights and setting the liability and jurisdiction rules under this Processor Standard.

2. Where European Personal Information is transferred under this Processor Standard by a European Group Member pursuant to a contract with a Client and where the Individual whose European Personal Information is transferred from Europe is unable to bring a claim against the Client because: (i) the Client has factually disappeared or ceased to exist in law or has become insolvent; and (ii)

no successor entity has assumed the entire legal obligations of the Client by contract or by operation of law, that Individual will have the right as a third party beneficiary to enforce Rules 1B, 2, 3, 4, 5, 9, 10, and 12, the right to easy access to information to which such Individuals are entitled regarding this Processor Standard and the right to enforce the provisions in this Section C(3),(4),(5),(6),(7),(8),(9) granting third-party beneficiary rights and setting the liability and jurisdiction rules under this Processor Standard.

3. The Individuals referred to in Sections C(2) and C(3) above are able to enforce the rights outlined in those sections by:

   (i) **making a complaint** to a competent Supervisory Authority in the European jurisdiction in which the alleged infringement took place, or in which the Individual works or habitually resides; and/or

   (ii) **bringing proceedings against the European Group Member** in the courts of the jurisdiction in which the relevant Client or that Group Member has an establishment, or in the jurisdiction in which the Individual has his or her habitual residence.

4. Where the Group Member and the Client are involved in the same Processing and are found responsible for any damage caused by such Processing, the Individuals referred to in Sections C(2) and (3) above will be entitled to claim compensation for the entire damage directly from the Group Member.

5. The Individuals referred to in Sections C(2) and (3) above may also seek appropriate redress from the European Group Member including the remedy of any breach of the Rules listed above, and where appropriate, compensation from that Group Member for any damage, whether material or non-material, suffered as a result of a breach of those Rules by:

   (i) any non- European Group Member; or

   (ii) by any Third Party Sub-Processor which is established outside Europe and which is acting on behalf of a Group Member,

   in accordance with the determination of the court or other competent authority.

6. The Company will assure that any necessary action is taken to remedy any breach of this Processor Standard by a non-European Group Member or any Third Party Sub-Processor which is established outside Europe and which is processing European Personal Information on behalf of a Client.

7. If a claim is made under this Section C in which any Individual has suffered damage as described above and where that Individual can demonstrate that it is likely that the damage has occurred because of a breach of the Rules described above or any of them, the Company has agreed that the burden of proof to show that a non-European Group Member (or any Third Party Sub-Processor which is established outside Europe and which is acting on behalf of a Group Member) is not responsible for the breach, or that no such breach took

place, will rest with the European Group Member transferring the European Personal Information to the Group Member (or Third Party processor) outside Europe.

8. In the event that the European Group Member referred 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 European Group Member.

9. The information to which Individuals are entitled regarding this Processor 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 prioritisation 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 harmonising 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:

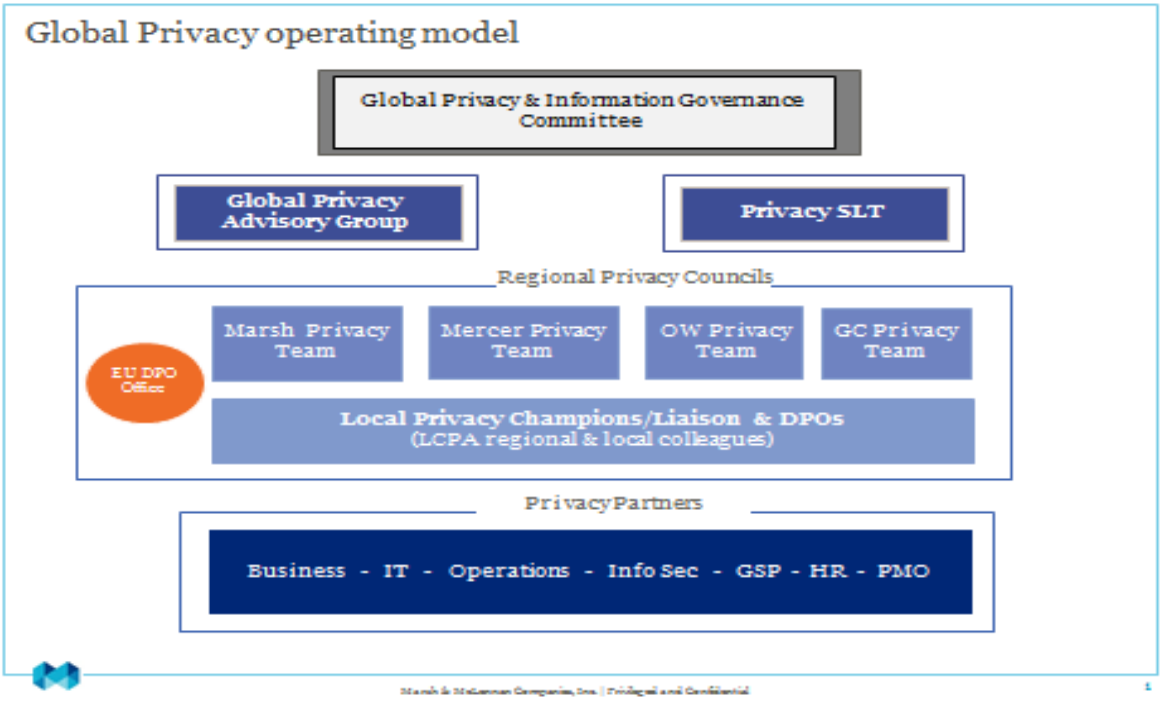
- EMEA
- Americas
- Asia Pacific

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 summarise 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.

(a) 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 - COMPLAINTS 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 the 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

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 2preferably 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.