MARSH & McLENNAN COMPANIES

BINDING CORPORATE RULES

CONTROLLER PRINCIPLES

INTRODUCTION

At Marsh & McLennan Companies (MMC), we respect and are committed to protecting the privacy, security and integrity of Personal Information[1] entrusted to us by our clients, business partners and colleagues.

We follow the core principles described below, and comply with applicable local privacy laws and regulations, including the European Data Protection Directive and equivalent member state legislation. Personal Information will be protected in accordance with that legislation regardless of geography or technology.

SCOPE

These principles apply to all Personal Information that originates from the European Economic Area (EEA)[2] and is processed by our legal entities and affiliates that entered into the MMC Intra-Group Agreement as participating in the MMC Binding Corporate Rules (BCRs) program (Group Members) for their own purposes, acting as a data controller.

PROCESSING PERSONAL INFORMATION

When processing Personal Information:

- We comply with all applicable legislation (for example, in Europe, local laws implementing the EU Data Protection Directive 95/46/EC as amended or replaced from time to time)that applies a higher standard of protection than these principles.
- We communicate to individuals, at the time their Personal Information is collected, how it will be used (usually by means of a fair processing statement). This information will be provided when Personal Information is obtained by us directly from the individual or as soon as practicable after that.
- We only obtain and use Personal Information for the purposes which are disclosed to individuals, or which are within their expectations as relevant to the products or

[1] Personal Information means any information relating to an identified or identifiable natural person in line with the definition of "personal data" in EU Directive 95/46/EC.

[2] References to European Economic Area (EEA) means all European Union countries, including Norway, Iceland and Lichtenstein.

services being offered. This disclosure will be made either to the individual whose data is collected or to the data controller who provides the data to us.

- We will only process Personal Information collected in Europe for an undisclosed or new purpose if we have a legitimate basis for doing so, consistent with the applicable law of the European country in which the Personal Information was collected.
- We will keep Personal Information accurate and up to date, and will only keep it for as long as is required and in accordance with record retention policies, procedures and schedules.
- We will follow our IT security policies, and implement appropriate technical and organizational measures to protect Personal Information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.
- We will comply with any relevant data breach notification requirements under applicable law.
- We will assure that service providers also adopt appropriate and equivalent security measures.

INDIVIDUAL RIGHTS

After an individual has satisfactorily authenticated their identity, they may:

- Access a copy of Personal Information held about them and certain other details such as their rights in relation to the Personal Information by submitting an email to mmcbcr@mmc.com.
- Request rectification, deletion, blocking or completion, as appropriate, of their Personal Information which is shown to be inaccurate or incomplete and, in certain circumstances, to raise an objection concerning the processing of their Personal Information.
- Object, free of charge, to the use of such Personal Information for direct marketing purposes and we will honor all such opt-out requests.
- Obtain an evaluation or decision which significantly affects them that is not solely based on automated processing of Personal Information, unless measures are taken to protect their interests, including providing them with an opportunity to understand the basis for the decision.

TRANS-BORDER TRANSFERS

We will not transfer Personal Information to other organizations outside the Group Members without assuring adequate protection for the information and taking appropriate steps, such as signing the standard contractual clauses or an equivalent data transfer

agreement, or obtaining the consent of individuals, in order to protect the Personal Information being transferred.

A Group Member acting as controller (the Exporting Entity) may transfer Personal Information originating in Europe to a Group Member outside Europe (the Importing Entity).

SENSITIVE PERSONAL INFORMATION

We will only use sensitive Personal Information if it is necessary. Sensitive personal information is information relating to an individual's racial or ethnic origin, political, religious or other beliefs, trade union membership, health, sex life and criminal convictions. Sensitive Personal Information will only be used where the individual's express consent has been obtained unless we have an alternative basis for doing so, consistent with the applicable law of the country where it was collected.

PRIVACY PROGRAM COMPLIANCE

We will have appropriate resources to oversee compliance with these principles throughout the Group Members. We have appointed our Global Chief Privacy Officer (GCPO) as the person to oversee compliance supported by a network of privacy leaders and privacy coordinators in the various Group Members' countries.

TRAINING AND AUDIT

We will provide appropriate training to colleagues who have permanent or regular access to, or who are involved in the collection or development of tools used to process Personal Information. Our Internal Audit department will conduct an annual audit in accordance with its procedures, or more frequently, at the request of the GCPO or the network of privacy leaders.

COMPLAINT HANDLING

Individuals, including colleagues, whose Personal Information is processed under the MMC BCRs may submit a complaint or query to mmcbcr@mmc.com. We are committed to promptly and appropriately investigating each privacy complaint submitted.

An individual may raise a complaint and/or bring proceedings where there is a breach of these Principles by Exporting or Importing Entities.

An individual may bring proceedings against the Exporting Entity if there is a breach by the Importing Entity. The individual may also bring a complaint to the data processing authority in the Exporting Entity’s country.

If an individual suffers damage, where that individual can demonstrate it is likely the damage occurred due to a breach of these Principles, then the burden of proof to show that no such breach took place will rest on the Exporting Entity.

COOPERATION WITH DATA PROTECTION AUTHORITIES

We will:

- Cooperate with European data protection authorities in relation to the BCRs
- Make colleagues available for dialogue with such authorities
- Actively review and consider any decisions made by relevant data protection authorities as they apply to BCRs and these Principles

UPDATES TO THESE PRINCIPLES

We will communicate any material changes to these principles as soon as is reasonably practical to the relevant European data protection authorities. At least annually, we will communicate any administrative changes or those that have resulted from a change of applicable law, to the relevant European data protection authorities. All changes will be communicated to Group Members through internal communications and to individuals and clients via our website.

WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE

Where a Group Member believes that other legislation prevents it from fulfilling its obligations under these principles or has a substantial effect on its ability to comply, the Group Member will promptly inform the GCPO, unless otherwise prohibited by law. The GCPO will make a decision on the action to be taken and, in case of doubt, consult the applicable data protection authority.

PROCESSOR PRINCIPLES

INTRODUCTION

At Marsh & McLennan Companies (MMC), we respect and are committed to protecting the privacy, security and integrity of Personal Information[3] entrusted to us by our clients, business partners and colleagues.

We follow the core principles described below, and comply with applicable local privacy laws and regulations, including the European Data Protection Directive and equivalent member state legislation. Personal Information will be protected in accordance with that legislation regardless of geography or technology.

SCOPE

These principles establish our obligations concerning the processing of Personal Information subject to the European Data Protection Directive or relevant Member State legislation when the Personal Information is collected by an external client ("Client") or by another Group Member (also referred to as "controller"). Where more than one Group Member is involved in the collecting and/or processing of the Personal Information, these principles assure consistent methods of processing are achieved.

Such Personal Information will be protected in accordance with that legislation regardless of geography or technology, when used by the Group Members.

These principles apply to all Personal Information that originates from the European Economic Area ("EEA")[4] and is processed by the Group Members acting as a data processor for and on behalf of a controller.

PROCESSING PERSONAL INFORMATION

When processing Personal Information:

- We will comply with all applicable legislation that applies a higher standard of protection than these principles.
- We will assist controllers with requests to comply with their obligations as controllers (e.g. Group Members will be transparent about sub-processor activities so that their controller client may inform the relevant individuals).

[3] Personal Information means any information relating to an identified or identifiable natural person in line with the definition of "personal data" in EU Directive 95/46/EC.

[4] References to EEA for the purposes of this document means all EU countries, including Norway, Iceland and Lichtenstein.

- The controller has a duty to explain to individuals, at the time their Personal Information is collected, how that information will be used (usually by means of a fair processing statement). Group Members will provide such information or, as agreed with the controller, to assist in fulfilling this obligation.
- We will only obtain and use Personal Information for the purposes which are agreed with the controller, or which are within their expectations as relevant to the products or services being offered. If we are unable to comply with the agreed assistance, the controller may suspend the transfer of data, or terminate the agreement, depending on the circumstances. In those situations, the Group Member should act in accordance with the controller's instructions and return and/or destroy the Personal Information. Where legislation prevents the Group Member from doing so, the Group Member will assure the continued confidentiality of the Personal Information and no longer process it.
- We will comply with requests from the controller to keep Personal Information accurate and up to date, and will only keep Personal Information for as long as required for the purposes for which it is collected and further processed. Where this cannot be achieved, the Group Member will promptly advise the controller, and assure that such Personal Information is no longer used in the provision of services.
- We will act in accordance with the instructions agreed with the controller, as to the exercising of individual rights. We will promptly notify the controller if we receive a subject access request from an individual.
- We will follow and implement the clear and specific obligations received from the controller to assure the implementation of proportionate technical and organizational measures to protect Personal Information against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access. We will notify a controller of any relevant data breach. Where the controller is another Group Member, we will comply with our internal breach notification procedure. Where the controller is a client, we will comply with the notification procedure agreed with the client.
- We will comply with the requirements agreed with the controller when considering appointing a sub-processor to process Personal Information on its behalf. Where a controller objects to the appointment, the Group Member may take steps as agreed with the controller. The Group Member will assure that sub-processors undertake to comply with the provisions which are consistent with (i) the terms in its contracts with its controllers and (ii) any additional requirements set out under the Processor Standards. The Group Member will only appoint sub-processors who have provided sufficient guarantees that the Group Member agreed with the controller, and in particular to have in place the appropriate technical and organizational measures to govern their processing of the relevant Personal Information.

PRIVACY PROGRAM COMPLIANCE

We will have appropriate resources to oversee compliance with these principles throughout the Group Members. We have appointed our Global Chief Privacy Officer ("GCPO") as the person to oversee compliance supported by a network of privacy leaders and privacy coordinators in the various Group Members' countries.

TRAINING AND AUDIT

We will provide training to colleagues who have permanent or regular access to Personal Information, or who are involved in the processing or development of tools used to process Personal Information. Our Internal Audit department will conduct an annual audit in accordance with its procedures, or more frequently at the request of GCPO or the network of privacy leaders.

COMPLAINT HANDLING

Individuals, including colleagues, whose Personal Information is processed under the MMC BCRs may submit a complaint or query to mmcbcr@mmc.com. We are committed to promptly and appropriately investigating each privacy complaint submitted.

COOPERATION WITH DATA PROTECTION AUTHORITIES

We will cooperate with European data protection authorities in relation to the MMC BCRs. We will make colleagues available for dialogue with authorities and actively review and consider any decisions made by data protection authorities and the views of the Article 29 Working Party, as applies to BCRs and these principles.

UPDATES TO THESE PRINCIPLES

We will communicate any material changes to the MMC BCRs as soon as reasonably practical to the UK Information Commissioner's Office ("ICO") and to any other relevant European data protection authorities. We will communicate any administrative changes or those that have resulted from a change of applicable law, to the ICO and relevant European data protection authorities at least once annually. All changes will be communicated to the Group Members through internal communications and to individuals and clients via our company website. We will maintain a log of any such changes.

WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE

Where a Group Member believes that the legislation prevents it from fulfilling its obligations under these Principles or has a substantial effect on its ability to comply, such Group Member will promptly inform the GCPO, unless otherwise prohibited by law. The GCPO will make a decision on the action to taken and, in case of doubt, consult the applicable data protection authority.

THIRD PARTY BENEFICIARY RIGHTS

In situations where Personal Information is transferred under these Principles, the individual whose Personal Information is transferred may be unable to bring a claim against the controller because:

- The controller no longer exists or has become insolvent; and
- No successor/replacement company has assumed the legal obligations of the controller.

In these situations, the individual has the following rights:

- To seek to enforce compliance with these Principles;
- To make a complaint to the European data protection authority in the country where
  - The Group Member who is processing the data is located; or
  - If no such Group Member exists, then where the Group Member in the country from where the personal information was transferred.
- To bring proceedings against the European Group Member acting as processor in either:
  - The jurisdiction from where the personal information was transferred; or
  - The European Member State where the individual resides.
- To receive compensation where appropriate, from the European Group Member acting as a processor, for damage suffered as a result of a breach of these Principles by:
  - Any non-European Group Member;
  - A third party data processor validly acting on behalf of the European Group Member and established outside the EEA;
  - In accordance with the valid ruling of the court of competent authority.
- To obtain a copy of the "Processor Standard" of the BCRs and intra-group agreement.

If an individual suffers damage, where that individual can demonstrate it is likely the damage occurred due to a breach of the Principles, then the burden of proof to show that no such breach took place will rest on the European Group Member transferring the Personal Information to the Group Member outside Europe.

We will take prompt action to remedy any breach of these Principles.