

EU BINDING CORPORATE RULES

Last Updated: 18 March 2021

CONTROLLER PRINCIPLES

INTRODUCTION

Marsh McLennan (MMC) respects and is committed to protecting the privacy, security and integrity of European Personal Information entrusted to us by our Clients, business partners and colleagues.

We follow the core principles described below (the Principles), and comply with European Data Protection Law. European Personal Information is protected in accordance with European Data Protection Law regardless of geography or technology.

SCOPE

These Principles apply to all European Personal Information that is Processed by Group Members participating in the MMC EU Binding Corporate Rules (EU BCR) program for their own purposes, acting as a Controller.

PROCESSING EUROPEAN PERSONAL INFORMATION

When Processing European Personal Information:

- We comply with any applicable legislation that requires a higher level of protection than the EU BCR.
- We explain to individuals, at the time their European Personal Information is collected, how that information will be Processed (usually by means of a fair processing statement). This information is provided at the point at which European Personal Information is obtained by us directly from the Individual, or as soon as practicable after that. Where we do not have a direct line of communication with Individuals, our Clients are contractually required to provide our fair processing information to Individuals.
- We only Process European Personal Information for those purposes which are disclosed to Individuals, or which are within their expectations as relevant to the products or services being offered. This disclosure is made either to the Individual whose data is collected or to the Controller who provides the data to us.
- We only Process European Personal Information for an undisclosed or new purpose if we have a legitimate basis for doing so, consistent with European Data Protection Law.
- We keep European Personal Information accurate, up to date, and only keep it for as long as is required and in accordance with record retention policies, procedures and schedules.
- We follow our IT security policies and implement appropriate technical and organisational measures to protect European Personal Information against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access.
- We comply with any relevant data breach notification requirements under European Data Protection Law.
- We assure that service providers also adopt appropriate and equivalent security measures.

INDIVIDUALS' RIGHTS

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

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

INTERNATIONAL TRANSFERS

We only transfer European Personal Information to Third Parties after taking appropriate steps, such as executing standard contractual clauses or an equivalent data transfer agreement, or obtaining the consent of individuals, in order to protect the European Personal Information transferred.

A Group Member acting as Controller (the Exporting Entity) may transfer European Personal Information to a Group Member outside Europe (the Importing Entity), under the EU BCR.

SPECIAL CATEGORY PERSONAL INFORMATION

We only use Special Category Personal Information if it is necessary. Special Category Personal Information is only Processed where the Individual's explicit consent has been obtained unless we have an alternative legal basis for Processing.

PRIVACY PROGRAM COMPLIANCE

We 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 provide appropriate training to colleagues who have permanent or regular access to, or who are involved in the Processing of, European Personal Information. Additionally, our EU BCR program is regularly audited by our internal audit department and/or our compliance teams.

COMPLAINT HANDLING

Individuals, including colleagues, whose European Personal Information is Processed under the EU BCR 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 Group Members;
- bring proceedings against the Exporting Entity if there is a breach by the Importing Entity; or

- make a complaint to a competent Supervisory Authority in the jurisdiction in which the alleged infringement took place, or in which the Individual works or habitually resides.

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.

CO-OPERATION WITH SUPERVISORY AUTHORITIES

MMC will co-operate with Supervisory Authorities in relation to the EU BCR and actively review and consider any decisions made by competent Supervisory Authorities on any European Data Protection Law issues that may affect the EU BCR. MMC will also review and consider the views of the European Data Protection Board (and any successor body) as outlined in its published guidance on BCRs.

UPDATES TO THESE PRINCIPLES

MMC reserves the right to modify its EU BCR. We will communicate any material changes to our lead supervisory authority, the Irish Data Protection Commission (Irish DPC), without undue delay, and via the Irish DPC, to any other competent Supervisory Authorities. Any material 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 legislation applicable to it prevents it from fulfilling its obligations under these Principles or has a substantial effect on the guarantees provided by the EU BCR, such Group Member will promptly inform Marsh & McLennan Ireland Limited as applicable and the GCPO, unless otherwise prohibited by law or a law enforcement authority. The GCPO will decide on the action to be taken and, in case of doubt, consult the Supervisory Authority with competent jurisdiction.

PROCESSOR PRINCIPLES

INTRODUCTION

Marsh McLennan (MMC) respects and is committed to protecting the privacy, security and integrity of European Personal Information entrusted to us by our Clients, business partners and colleagues.

We follow the core principles described below (the Principles), and comply with European Data Protection Law. European Personal Information is protected in accordance with European Data Protection Law regardless of geography or technology.

SCOPE

These Principles establish our obligations concerning the processing of European Personal Information subject to European Data Protection Law when the European Personal Information is collected by a Client or by another Group Member (also referred to as a Controller). Where more than one Group Member is involved in the Processing of the European Personal Information, these Principles assure consistent methods of Processing are achieved. Such European Personal Information will be protected in accordance with European Data Protection Law regardless of geography or technology, when used by the Group Members.

These Principles apply to all European Personal Information that is Processed by Group Members when acting as a Processor for and on behalf of a Controller.

PROCESSING EUROPEAN PERSONAL INFORMATION

When Processing European Personal Information:

- We comply with any applicable legislation that requires a higher level of protection than the EU BCR.
- We 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).
- The Controller has a duty to explain to Individuals, at the time their European Personal Information is collected, how that information will be Processed (usually by means of a fair processing statement). Group Members will provide such information or, as agreed with the Controller, assist in fulfilling this obligation.
- We only obtain and use European Personal Information for those purposes agreed with the Controller, or within their expectations as relevant to the products or services offered. If we are unable to comply with the agreed assistance, the Controller may suspend the transfer of European Personal Information and/or terminate the contract, depending upon the terms of its contract with the Group Member. In those situations, the Group Member will act in accordance with the contract and the Controller's instructions and, where required, return and/or destroy the European Personal Information. Where European Data Protection Law prevents the Group Member from doing so, the Group Member will assure the continued confidentiality of the European Personal Information and no longer Process it.
- We comply with requests from the Controller to keep European Personal Information accurate, up to date and will only keep European 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 European Personal Information is no longer used in the provision of services.
- We act in accordance with the instructions agreed with the Controller, as to the exercising of

individual rights. We promptly notify the Controller if we receive a subject access request from an Individual.

- We follow and implement the clear and specific obligations received from the Controller to assure the implementation of proportionate technical and organisational measures to protect European Personal Information against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access. We notify Controllers of any relevant data breach. Where the Controller is another Group Member, we comply with our internal breach notification procedure. Where the Controller is a Client, we comply with the notification procedure agreed with the Client.
- We comply with the requirements agreed with the Controller when considering appointing a Sub-Processor to Process European 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:
 - the terms in its contracts with its Controllers; and
 - any additional requirements set out under the EU BCR.

The Group Member only appoints Sub-Processors who have provided sufficient guarantees in respect of the commitments made by the Group Member in the EU BCR. In particular such Sub-Processors must be able to provide appropriate and equivalent technical and organisational measures to govern their Processing of the European Personal Information.

PRIVACY PROGRAM COMPLIANCE

We 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 provide appropriate training to colleagues who have permanent or regular access to, or who are involved in the Processing of European Personal Information. Additionally, our EU BCR program is regularly audited by our internal audit department and/or our compliance teams.

COMPLAINT HANDLING

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

COOPERATION WITH SUPERVISORY AUTHORITIES

MMC will co-operate with Supervisory Authorities in relation to the EU BCR and actively review and consider any decisions made by competent Supervisory Authorities on any European Data Protection Law issues that may affect the EU BCR. MMC will also review and consider the views of the European Data Protection Board (and any successor body) as outlined in its published guidance on BCRs.

UPDATES TO THESE PRINCIPLES

MMC reserves the right to modify its EU BCR. We will communicate any material changes to our lead supervisory authority, the Irish Data Protection Commission (Irish DPC), without undue delay, and via the Irish DPC, to any other competent Supervisory Authorities. Any material 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 legislation applicable to it prevents it from fulfilling its obligations under these Principles or has a substantial effect on the guarantees provided by the EU BCR, such Group Member will promptly inform Marsh & McLennan Ireland Limited as applicable and the GCPO, unless otherwise prohibited by law or a law enforcement authority. The GCPO will decide on the action to take and, in case of doubt, consult the applicable Supervisory Authority with competent jurisdiction.

THIRD PARTY BENEFICIARY RIGHTS

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

- The Controller has factually disappeared or ceased to exist in law or has become insolvent; and
- No successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law.

In these situations, the Individual has the following rights:

- To seek to enforce compliance with these Principles;
- To make 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;
- To bring proceedings against the European Group Member acting as Processor in either:
 - The courts of the jurisdiction in which the relevant Controller or that Group Member has an establishment; or
 - The jurisdiction in which the Individual has his or her habitual residence;
- To receive compensation, where appropriate, from the Group Member acting as a Processor, for any damage, whether material or non-material, suffered as a result of a breach of these Principles by:
 - any non-European Group Member;
 - a Third Party Sub-Processor validly acting on behalf of the Group Member and established outside Europe; or
 - in accordance with the valid determination of the court or other competent authority.
- To obtain a copy of the “Processor Standard” of the EU BCR and intra-group agreement.

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

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

DEFINITIONS

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

Europe means the European Economic Area (EEA) and Switzerland.

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

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

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 EU BCR program.

Personal Information means any information relating to an identified or identifiable natural person.

Special Category Personal Information is information relating to an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation.

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