TMF GROUP

Global reach
Local knowledge

Binding Corporate Rules for Processing Customer Personal Data (Processor)

June 2015

tmf-group.com

TMF GROUP

Global reach
Local knowledge

Binding Corporate Rules for Processing Customer Personal Data (Processor)

Introduction

These BCRs define the standards applicable to TMF Group B.V. and its affiliates (together "**TMF**" or "**TMF Group**" and each a "**TMF Affiliate**") in relation to the Processing of personal data on behalf of TMF clients. In such case, TMF will be the Processor and the TMF client will be the Controller.

"**Affiliate**" means with respect to any specified person or entity, any other person or entity directly or indirectly controlling or controlled by or under direct or indirect common control with such specified person or entity. For the purpose of this definition, "control", when used with respect of any specified person or entity means the power to direct or cause the direction of the management or policies of such person or entity, whether through ownership of voting securities or by contract or otherwise. The terms "controlling" and "control" have meaning correlative to the foregoing. Excluded from the definition of Affiliates are the shareholding companies above TMF Group B.V.

A list of TMF Affiliates bound to these BCRs is available on request from the Chief Privacy Officer. The request must be addressed to TMF Group B.V., Luna ArenA, Herikerbergweg 238, 1101 CM Amsterdam , the Netherlands or P.O. Box 723393, 1100 DW Amsterdam Zuidoost, the Netherlands, or to grouplegal@tmf-group.com.

The objective of these BCRs is to provide adequate protection for the transfers and Processing of Personal Data by TMF Affiliates in their role as Processor or Sub-Processor.

The board of management of TMF will ensure compliance with the described rules. The BCRs are incorporated by reference into TMF's global Code of Conduct which all TMF employees are required to acknowledge and comply with. All TMF Affiliates will respect these BCRs. All persons who have access within TMF to Personal Data must comply with these BCRs.

1. Scope

The transfer of Personal Data by TMF consists of the making accessible of a number of databases to TMF employees in a large number of countries, both in- and outside the European Economic Area ("**EEA**"). These databases contain information of clients, including employees of clients, and other Data Subjects, as part of TMF's regular business activities.

The Personal Data covered by these BCRs is Processed and transferred by TMF Affiliates as Processors for the purposes of client services contracts execution: actual rendering of payroll, human resource administration of clients, bookkeeping of clients and other services, pursuant to contractual terms and conditions agreed in writing with the client. This Processing will take place according to the instructions of the client and the Service Agreement.

Personal Data may also include Personal Data of employees of clients, i.e. name, address, telephone number, e mail address, date of birth, marital status, (tax and social) identification numbers, salary and other benefits, taxes and social premiums (rates, tariffs) of individuals employed by clients of TMF and financial information about transactions (to be) conducted by clients.

Personal Data is either collected from the Data Subject or the employer of the Data Subject.

TMF will apply the BCRs to any and all intra-group transfers and Processing of Personal Data within TMF, where TMF acts as a Processor of Personal Data of Clients from the EEA or Switzerland as well as of Personal Data of affiliates of non-European Clients in the EEA or Switzerland. With respect to non-European Personal Data, these BCRs are considered a guideline for TMF staff regarding the Processing of such Personal Data, and will only be binding on TMF and its staff where TMF has specifically agreed with the Client to the applicability of these BCRs to such Data.

The capitalized terms listed below have the following meaning in the BCRs:

a. "**Personal Data**" shall mean any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity;
b. "**Controller**" shall mean the TMF client who alone or jointly with others determines the purposes and means of the Processing of Personal Data;
c. "**Processor**" shall mean the TMF Affiliate who Processes Personal Data on behalf of the Controller in the course of the services provided to such Controller;
d. "**Processing**" shall mean any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;
e. "**Third Party**" shall mean any natural or legal person, public authority, agency or any other body other than the Data Subject, the Controller, TMF or the persons who, under the direct authority of the Controller or TMF, are authorized to Process the Personal Data;
f. "**Data Protection Authority**" shall mean the authority, which is responsible for monitoring the application within its territory of personal data protection laws.
g. "**EU Headquarters**" means the statutory seat and registered address of TMF Group B.V. at Luna ArenA, Herikerbergweg 238, 1101 CM Amsterdam, the Netherlands.
h. "**Sensitive Data**" shall mean personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the Processing of data concerning health or sex life.
i. "**Sub-Processor**" shall mean any TMF Affiliate assisting the Processor in the provision of the TMF services as well as any Third Party engaged by TMF to assist TMF in the provision of the Services in countries where TMF does not have a presence or to provide information technology, administrative support or consultancy services to TMF.

2. Service Agreement

TMF will enter into a Processor contract with the Controllers regarding its Processing of Personal Data for the purposes of providing the TMF services. These contracts will be referred to here as the '**Service Agreements**'.

All relevant parts of these BCRs shall be converted into contractual provisions in the Service Agreement. These BCRs shall be attached to the Service Agreement with Clients from the EEA or Switzerland or Clients with affiliates in such countries as an annex and shall thereby become binding on the Controller.

3. Transfers to Third Parties and Sub-Processors

A TMF Affiliate may transfer Personal Data to a Third Party:

a. where so authorized or so instructed by the Controller in writing;
b. if such Third Party is a Sub-Processor and the transfer is necessary for the provision of the services of such Sub-Processor;
c. as necessary to comply with a legal obligation to which the Controller or the Processor is subject;
d. to protect TMF's legal rights;
e. in an emergency where the health or security of a Data Subject is endangered; or
f. as requested by the Data Subject.

Sub-Processors may Process the Personal Data only in accordance with TMF's instructions and to the extent necessary for the purpose of performing the services specified in the contract between TMF and the Sub-Processor.

The authorization or instruction of the Controller for the sub-Processing shall be obtained through the Service Agreement. Upon request, TMF will provide the Controller with the name and address of the Sub-Processor.

TMF will enter into Processing agreements with the sub-Processors. All relevant parts of these BCRs shall be converted into contractual provisions of such Processing agreement. Such agreements will provide for a level of protection substantially similar or higher than the protection afforded by applicable law or the Service Contract. Where a general authorization for Sub-Processing was given by the Controller, TMF will inform the Controller of any intended changes concerning the addition or replacement of a Sub-Processor in a timely fashion.

4. Purpose Limitation

Personal Data will be Processed and transferred fairly and in accordance with the Data Subject's rights as described in these BCRs or as provided by law.

Personal Data will only be transferred and Processed on behalf of the Controller and in compliance with the Controller's instructions and the Service Agreement (the **"Authorized Purposes"**) and will not be further Processed in a way that is incompatible with the Authorized Purposes.

Upon termination of the Service Agreement, TMF shall, at the choice of the Controller:

a. destroy all the Personal Data Processed and the copies thereof and certify to the Controller that it has done so; or
b. return all the Personal Data Processed and the copies thereof to the Controller,

unless any applicable law, regulation, supervisory or regulatory body or TMF's internal compliance requirements prevents it from returning or destroying all or part of the Personal Data. In the latter case, TMF will inform the Controller and warrant that it will guarantee the confidentiality of the Personal Data and will not Process the Personal Data for the Authorized Purposes or any other purposes except for storage, the protection of the Personal Data or as required by applicable law.

The obligation to destroy or return Personal Data does not apply to any notes, analyses, memoranda, minutes or other internal corporate documents, prepared by or on behalf of TMF which are based on, derived from, contain or otherwise make reference to Personal Data. Furthermore, TMF is entitled to retain copies of any computer records and files containing Personal Data which have been created pursuant to automatic electronic archiving and back-up procedures and which is not immediately retrievable as part of day-to-day business.

5. Transparency and information right

In order to make the BCRs accessible to Data Subjects, TMF may publish the BCRs and any appendices or amendments on the TMF website, make the BCRs available to Data Subjects on request (directly or via the client) and refer to the BCRs in services offerings, client acceptance procedures and commercial contracts.

In order to make the BCRs accessible to Controllers, the Service Agreement will include a reference to the applicability of the BCRs and the BCRs will be made available to the Controller on request.

6. Cooperation with the Controller

TMF will co-operate and assist the Controller to comply with relevant data protection laws in a reasonable time and to the extent reasonably possible.TMF will help, assist and inform the Controller insofar as is reasonably necessary to comply with the rights of the Data Subjects regarding access, rectification, erasure and blocking of Personal Data. In particular:

a. TMF will execute any necessary measures requested by the Controller in order to have the Personal Data updated, corrected or deleted;
b. TMF will execute any necessary measures requested by the Controller in order to have the Personal Data deleted or made anonymous from the moment the Processing of Personal Data is not necessary anymore.

If a Data Subject files a request regarding the Processing of his/her Personal Data with a TMF Affiliate acting as a Processor, the Local Privacy Officer shall communicate the request without delay to the Controller. The Local Privacy Officer is not obligated to handle the request, unless the Controller has disappeared factually or has ceased to exist in law or has become insolvent.

7. Automated individual decisions

No evaluation of or decision about the Data Subject which significantly affects him/her will be based solely on automated Processing of their Personal Data, unless that decision:

a. is taken in the course of entering into or performance of a contract, provided the request for entering into or the performance of the contract, lodged by the Data Subject has been satisfied or that there are suitable measures to safeguard his/her legitimate interests, such as arrangements allowing him/her to put his point of view; or
b. is authorized by law.

8. Security and confidentiality

TMF is committed to taking appropriate reasonable technical, physical and organizational measures to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access (in particular where the Processing involves the transmission of Personal Data over a network) and against all other unlawful forms of Processing.

TMF will implement security measures in accordance with TMF Information and Security policies, the Cloud policy and the Service Agreement.

TMF shall, to the extent permitted by law, take reasonable steps to ensure the reliability of employees who have access to the Personal Data. TMF shall only authorize its personnel to access the Personal Data for the Authorized Purposes or where there is a legitimate business, legal or regulatory reason to do so.

Security and protection are described in the Security and Business Continuity Outline and may be further detailed in the Service Agreement.

In case of a security breach of which TMF has knowledge, and to the extent that the Personal Data of the Controller will be affected, TMF will immediately inform the Controller of the nature of the breach, an estimation of the number of the Data Subjects involved, and, where possible, their names.

9. Training and audit program

TMF will provide training on the BCRs to all personnel who have permanent or regular access to Personal Data, are involved in the collection of Personal Data or in the development of tools used to Process Personal Data.

TMF will develop an e-program to test employees on awareness and compliance with BCRs. TMF has implemented an e-learning system, which will enable TMF and its Affiliates to develop and deploy customized training courses. It also is a learning management system able to host and support the tracking of TMF data protection training worldwide.

Besides the e-learning tool, presentations on data protection will be scheduled to regional management of TMF.

TMF will carry out data and system audits on a regular basis or on specific request from the Chief Privacy Officer or any other competent function in the organization.

The audit program covers all aspects of the BCRs including methods of ensuring that corrective actions will take place. The results of all audits are reported to the Chief Information Security Officer and to the Chief Privacy Officer of TMF Group. An executive summary of the results will be made available to the Controller, upon request. TMF will provide a copy of the audits upon request of the Data Protection Authorities competent for the Controller.

In addition to the data and system audits, the internal auditing department of TMF will perform an audit on a regular basis. For the countries where TMF is regulated under financial service laws, the audit will be performed annually. In all other countries, the audit will be performed every 3 years.

Data Protection Authorities have the power to carry out an audit if required and legally possible. Each member of TMF Group accepts that they may be audited by the competent Data Protection Authorities and that they will abide by the advice of the Data Protection Authorities.

All TMF Affiliates Processing the Personal Data of a specific Controller will accept, at the request of that Controller, an audit on their facilities for Processing of Personal Data to be carried out by an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality and selected by the Controller and approved by the Processor (which approval shall not unreasonably be withheld or delayed) and, where applicable, in agreement with the Data Protection Authority. The audit will be carried out by the independent auditor in close cooperation with the Chief Information Security Officer. TMF is entitled to request a reasonable compensation for the costs of the audit incurred by TMF, to be paid by the Controller.

10. Compliance and supervision of compliance

TMF will appoint appropriate staff with top management support to oversee and ensure compliance with the rules. Structure, roles and responsibilities have been determined.

Group Head Legal and Risk Management: responsible for management of global compliance.

Chief Information Security Officer: annually reports on data and system security at a global level, responsible for data and system audits, reports in this respect to the Group Head Legal and Risk Management and advises the Chief Privacy Officer.

Group Compliance director: heads the Compliance department of TMF Group which task and responsibility is the execution of “know your client” identification procedures for accepting clients and specific client compliance procedures and reports to the Group Head Legal and Risk Management.

Chief Privacy Officer: deals with Data Protection Authorities’ investigations, annually reports to the Group Head Legal and Risk Management on compliance of the BCRS, ensures compliance of the BCRs at a global level.

Local Privacy Officer: responsible for handling local complaints from Data Subjects, reporting major privacy issues to the Chief Privacy Officer and for ensuring compliance of the BCRs at a local level.

11. Enforcement rights and mechanisms

Complaints

Data Subjects may file a complaint regarding the Processing of their Personal Data with the appropriate Local Privacy Officer. The Local Privacy Officer shall communicate the complaint without delay to the Controller. The Local Privacy Officer is not obligated to handle the complaint.

If the Controller has factually disappeared or ceased to exist in law or has become insolvent, the Local Privacy Officer shall:

a. notify the Chief Privacy Officer;
b. initiate an investigation;
c. when necessary, advise the business on the appropriate measures for compliance and monitor, through completion, the steps designed to achieve compliance;
d. send a response to the Data Subject within 14 days after receiving the complaint. This period may be extended in more complex cases (maximum period will be 3 months). The Data Subject will be notified of the extended period.

Complaints must be addressed to the Local Privacy Officer of the TMF Affiliate which did not comply with the BCRs.

A Data Subject may file a complaint with the Chief Privacy Officer if:

a. the resolution of the complaint by the Local Privacy Officer is unsatisfactory to the Data Subject (e.g., the complaint is rejected);
b. the Data Subject has not received a response within 14 days; or
c. the time period provided to the Data Subject is, in light of the relevant circumstances, unreasonably long and the Data Subject has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response.

The procedure described above shall also apply to complaints filed with the Chief Privacy Officer.

Complaints filed with the Chief Privacy Officer must be addressed to TMF Group B.V., Luna ArenA, Herikerbergweg 238, 1101 CM Amsterdam, the Netherlands or P.O. Box 23393, 1100 DW Amsterdam Zuidoost, the Netherlands, or grouplegal@tmf-group.com and telephone +31 (0) 20 575 5600 to the attention of the Chief Privacy Officer.

If the complaint is considered justified, TMF will remedy any potential faults, errors or omissions and will provide an explanation to the Data Subject. If the Data Subject is not satisfied with the remedy provided by TMF, the Data Subject may enforce the BCRs in accordance with the below.

Enforcement by the Data Subject

These BCRs grant rights to Data Subjects to enforce the rules as third-party beneficiaries.

The processes described in these BCRs supplement any other remedies and dispute resolution processes provided by TMF or available under applicable law. Hence, the Data Subject may at any time - without lodging a prior complaint with the Local or Chief Privacy Officer of TMF - lodge a complaint before the Data Protection Authority or court competent for the Controller in the EEA. If this is not possible because the Controller has factually disappeared or ceased to exist in law or has become insolvent, the Data Subject may take action before the Data Protection Authority or the court competent for the EU Headquarters or the TMF Affiliate in the EEA which acted as the Processor at the origin of the transfer. If there is a successor entity to the Controller which has assumed the entire legal obligations of the Controller by contract or by operation of law, the Data Subject can enforce his/her rights against the successor entity.

If the above is not possible, the Data Subject shall be entitled to lodge a complaint to the court of his/her place of residence.

Enforcement by the Controller

The Controller shall have the right to enforce the BCRs against a TMF Affiliate for breaches of the Service Agreement or the BCRs that the TMF Affiliate has caused. The Controller's rights shall cover the judicial remedies and the right to receive compensation.

If the Service Agreement or the BCRs were breached by a TMF Affiliate or a sub-Processor established outside the EEA, EU Headquarters will accept liability as set out in the section below.

12. Liability

EU Headquarters is responsible for and will take the necessary action to remedy the acts of TMF Affiliates outside the EEA or breaches caused by sub-Processors established outside the EEA. EU Headquarters will pay compensation for any damages resulting from the violation of the BCRs by any TMF Affiliate or sub-Processor and has sufficient assets to do so.

EU Headquarters accepts liability as if the violation had taken place by it in the Member State in which it is based.

If the Data Subject or the Controller can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of the breach of the BCRs, EU Headquarters bears the burden of proof to demonstrate that the TMF Affiliate or sub-Processor is not liable for the violation resulting in the damages claimed by the Data Subject or the Controller. If the EU Headquarters can prove that the TMF Affiliate or sub-Processor is not liable for the violation, it may discharge itself from any responsibility. EU Headquarters may not rely on a breach by a sub-Processor in order to avoid its own liabilities.

13. Mutual assistance and cooperation with Data Protection Authorities

All TMF Affiliates will cooperate and assist each other to handle a request or complaint from a Data Subject or Controller or an investigation or inquiry by Data Protection Authorities.

All TMF Affiliates will respond diligently and appropriately to requests from all Data Protection Authorities. All TMF Affiliates will abide by the advice of the Data Protection Authorities on any issues regarding the interpretation of the BCRs. All TMF Affiliates will inform the EU headquarters of any requests and advices from Data Protection Authorities. The Chief Privacy Officer will manage requests from and investigations by the Data Protection Authorities.

14. Updates of the rules

TMF reserves the right to modify these BCRs as needed, for example, to comply with changes in laws, regulations, TMF practices and procedures or requirements imposed by Data Protection Authorities.

Any substantive changes to these BCRs shall be reported to the affected TMF Affiliates. The relevant Data Protection Authorities will receive this information annually.

The Controller will be informed at least 60 days in advance of any substantive changes to these BCRs taking effect and any changes that affect the Processing conditions. In the event of detrimental effects to the Controller, the Controller may object to the change or terminate the Service Agreement before the change enters into force.

Where required by law, TMF will submit the BCRs to the Data Protection Authorities for renewed approval.

The Chief Privacy Officer will keep a fully updated list of the entities bound by the BCRs, including the TMF Affiliates and the sub-Processors and will keep track of and record any updates to the rules. An updated list of the entities shall be reported to the relevant Data Protection Authorities annually.

No Personal Data will be transferred to a new TMF Affiliate until the Affiliate is effectively bound by the BCRs and can deliver compliance.

15. Relationship between national laws and the BCRs

These BCRs are designed to provide a minimum standard with respect to the protection of Personal Data for every TMF Affiliate. Where national laws require a higher level of protection than that provided for in these BCRs, TMF will Process the Personal Data in accordance with these national laws.

If an TMF Affiliate has reason to believe that (future) legislation applicable to it prevents the Affiliate from fulfilling its obligations under the BCRs or the Service Agreement and has substantial effect on the guarantees provided by the rules, it will promptly inform the Controller, EU Headquarters and the Data Protection Authority competent for the Controller. The Controller will be entitled to suspend the transfer of Personal Data and/or terminate the Service Agreement.

Any legally binding request for disclosure of Personal Data by a law enforcement authority shall be communicated to the Controller unless prohibited by law. In any case, the request for disclosure will be put on hold and the Data Protection Authority competent for the Controller and the lead Data Protection Authority for the BCRs will be clearly informed.

16. Effective date

June 16, 2015