

TMF
GROUP

Global reach
Local knowledge

PERSONAL DATA PROTECTION POLICY

Client Personal Data Processing by TMF Group

June 2021 | Version 2.2



tmf-group.com



TABLE OF CONTENTS

GENERAL NOTICE	3
1. INTRODUCTION AND SCOPE	5
2. DEFINITIONS	6
3. PERSONAL DATA PROCESSED BY TMF	7
4. USE OF PERSONAL DATA	7
5. SUBPROCESSING	8
6. CONFIDENTIALITY AND SECURITY	8
7. CO-OPERATING WITH REQUESTS OF THE CLIENT	9
8. DELETION OR RETURN OF CLIENT PERSONAL DATA	10
9. INCIDENT MANAGEMENT	10
10. INTERNATIONAL TRANSFERS OF CLIENT PERSONAL DATA	11
11. LIABILITY	12
12. CONTACT US	13
REFERENCE TO ASSOCIATED DOCUMENTS	14
REVISION HISTORY AND RECORDS	14



GENERAL NOTICE

This document falls under TMF Group Legal and Risk control. The following applies to this document:

- ① This document is controlled as part of TMF Group Legal and Risk, governance control.
- ① No changes to this document are permitted without formal approval from the document owner.
- ① This document is classified, version controlled and regularly reviewed.
- ① Any questions regarding this document should be raised to the owner.
- ① Distribution, modifications and access must be addressed based on TMF Group's information classification.
- ① The version of this document can be found on the cover page.
- ① Revision details are described below.
- ① This document may be available in various languages; however the version in the English language will prevail.

CLASSIFICATION

Public

GOVERNANCE

Owner	Chief Privacy Officer
Approver	Risk and Compliance Committee of the Board
Sponsor	CFO

CONTACT POINT

Contact	dataprotection@tmf-group.com
----------------	--------------------------------------------------------------------------------

REVIEW

Period	Annual
Last review	June 2021
Status	Final
Approval on	03 June 2021
Effective date	03 June 2021



1. INTRODUCTION AND SCOPE

This Personal Data Protection Policy ("**Policy**") describes the privacy practices of TMF regarding the Processing of Personal Data of the directors, officers and employees and – to the extent applicable – the customers of the Client and/or the relevant Client Affiliates, as part of the provision of TMF Services to its Clients. This Personal Data can be stored on TMF systems, Client systems or third-party systems to which TMF is provided access to for the provision of Services. Where TMF provides Services to its Clients, TMF will be acting as Processor and the Client will be acting as Controller.

This Policy applies globally to any and all Services provided by TMF to its Clients under the Service Agreements, executed on or after the effective date of this Policy.

TMF Processes Personal Data on behalf of the Client in accordance with Data Protection Laws. Insofar necessary, the Service Agreement will be supplemented with an Addendum to set out any additional matters that are specific to the Client and cannot be regulated in this Policy.

This Policy does not apply to the collection of Personal Data through our website or through cookies with respect to which Personal Data TMF can be considered Controller; we refer to our separate [Website Privacy Statement](#) and [Cookies Policy](#) for more information in this regard.

This Policy is available through the TMF Group website at the following link: <https://www.tmf-group.com/en/legal/data-protection/>. TMF reserves the right to update this Policy without consulting or pre-informing its Clients. Notwithstanding the foregoing, the version of the Policy that applies and will continue to apply to a particular Service Agreement will be the version of the Policy that is in effect at the time of the effective date of such Service Agreement, unless amendments are required to comply with Data Protection Laws in which case the most recent version of the Policy published on the website shall apply.

2. DEFINITIONS

The capitalized terms listed below have the follow meaning in this Policy:

- a. **“Client”** means the counterparty to the Service Agreement with TMF;
- b. **“Client Affiliate”** means any legal entity affiliated to the Client;
- c. **“Client Data Subjects”** shall mean the former and current directors, officers and employees and customers of the Client and Client Affiliates;
- d. **“Controller”** shall mean the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data;
- e. **“Data Protection Audit”** means audits, including data protection compliance questionnaires, carried out by the Client or a third-party on behalf of the Client, with the objective to verify TMF compliance with the data protection obligations stated in the Service Agreement and this Policy.
- f. **“Data Protection Laws”** means in relation to any Personal Data which is Processed in the performance of the Service Agreement, the General Data Protection Regulation (EU) 2016/679 (**“GDPR”**) together with all implementing laws and any other applicable data protection, privacy laws or privacy regulations;
- g. **“Personal Data”** means any information through which a Client Data Subject can be identified directly or indirectly;
- h. **“Personal Data Breach”** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.
- i. **“Processing”** means any operation or set of operations which is performed upon Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
- j. **“Processor”** shall mean the party, which Processes Personal Data on behalf of the Controller;
- k. **“Services”** means services TMF provides to the Client under the Service Agreement;
- l. **“Service Agreement”** means any written contract, any written statement of work, or any other written binding agreement, including any annexes thereto, between TMF and the Client;
- m. **“Subprocessor”** means any data processor appointed by Processor to process Personal Data on behalf of the Controller;

- n. “**TMF**” means the TMF Affiliate that is the contracting entity to the Service Agreement;
- o. “**TMF 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. Specifically excluded from this definition are the shareholding companies controlling TMF Group B.V.

3. PERSONAL DATA PROCESSED BY TMF

The details of the Personal Data that will be Processed by TMF on behalf of the Client, including the duration, purpose and types and categories of Personal Data, as well as Subprocessors, if any, will be set out on TMF Group website pages **Details of Processing** (<https://www.tmf-group.com/en/legal/data-protection/details-of-processing>) respectively **Subprocessors** (<https://www.tmf-group.com/en/legal/data-protection/subprocessors>).

4. USE OF PERSONAL DATA

TMF shall not process, transfer, modify, amend or alter the Personal Data or disclose or permit the disclosure of the Personal Data to any third party other than:

- Ⓞ as necessary to process Personal Data to provide the Services and/or otherwise in accordance with the documented instructions of Client, or
- Ⓞ as required to comply with Data Protection Laws or other laws to which TMF is subject, in which case TMF shall (to the extent permitted by law) inform Client of that legal requirement before processing the Personal Data.

In addition, TMF is allowed to use aggregated data – to the extent this can no longer be considered Personal Data - for analysing purposes, for website and for internal operations,



including troubleshooting, data analysis, testing, research, for statistical purposes and for improving the quality of its Services.

5. SUBPROCESSING

TMF may be required to appoint certain third parties, including TMF Affiliates, to provide part of the Services to the Client or assist with providing technical support, such as IT service providers or other suppliers. By signing the Service Agreement, the Client authorises TMF to subcontract the Processing of Personal Data to Subprocessors in the relevant countries where the Services will be rendered as listed on **Subprocessors** (<https://www.tmf-group.com/en/legal/data-protection/subprocessors>) page. Subprocessors are in each case subject to the terms between TMF and the Subprocessor which are no less protective than those set out in this Policy and the Service Agreement. TMF will inform the Client of the details of such Subprocessor(s) upon written request from the Client. TMF will inform the Client in advance of any intended changes concerning the addition or replacement of Subprocessors and thereby give the Client the opportunity to object to such changes. If the Client does not object in writing within fifteen (15) days of receipt of the notice, the Client is deemed to have accepted the new Subprocessor. If the Client does object in writing within fifteen (15) days of receipt of the notice, TMF and the Client will discuss possible resolutions within a reasonable timeframe and without detriment to the Parties and to their compliance with each of their respective obligations set forth in the Services Agreement.

6. CONFIDENTIALITY AND SECURITY

TMF shall keep the Personal Data confidential and will ensure its staff and Subprocessors are bound by the same confidentiality obligation. TMF shall implement appropriate technical and organisational measures to ensure a level of security of the Personal Data appropriate to the risk required pursuant to applicable Data Protection Laws and, where the Processing concerns personal data of EU residents, shall take all measures required pursuant to article 32 GDPR. In assessing the appropriate level of security, TMF shall take account in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed. The security measures are further described and specified in the document "[Statement of Continuity](#)", which is published on the TMF Group website (<https://www.tmf-group.com/en/legal/data-protection/>) and forms an integral part of



this Policy. Any subsequent versions of the document Statement of Continuity shall be applicable to the Services Agreement and its content will be no less stringent than its previous version.

7. CO-OPERATING WITH REQUESTS OF THE CLIENT

TMF shall, upon request and to the extent required under Data Protection Laws, co-operate with requests of the Client that relate to the Processing of Personal Data. In particular, TMF shall co-operate with requests that relate to Client Data Subject rights, Data Protection Impact Assessments and audit rights as described below.

Client Data Subject rights: TMF shall co-operate as requested by the Client to enable the Client to comply with its obligations with any exercise of rights by a Client Data Subject in respect of Personal Data and assist Client in its compliance with any assessment, enquiry, notice or investigation as required under Data Protection Laws. Provided in each case that the Client shall reimburse TMF in full for all costs (including for internal resources and any third party costs) reasonably incurred by TMF performing its obligation to assist Client in its compliance under this section.

Data Protection Impact Assessment: TMF shall provide reasonable assistance to the Client with any data protection impact assessments which are required under Data Protection Laws, including Article 35 GDPR, and with any prior consultations to any Supervisory Authority of the Client which are required under Data Protection Laws, including Article 36 GDPR, in each case in relation to Processing of Personal Data by TMF on behalf of the Client and taking into account the nature of the processing and information available to TMF.

Audit rights: On reasonable request and notice, TMF will co-operate in the conduct of any Data Protection Audit or inspection, reasonably necessary to demonstrate TMF's compliance with the processor obligations laid down in Data Protection Laws and this Policy related to the Service Agreement, provided always that this requirement will not oblige TMF to provide or permit access to information concerning: (i) TMF internal pricing information; (ii) information relating to TMF's other Clients; (iii) any of TMF non-public external reports, or (iv) any internal reports prepared by TMF's internal audit function. The Client shall avoid causing any damage, injury or disruption to TMF's equipment, personnel and business in the course of such Data Protection Audit or inspection. A maximum of one Data Protection Audit may



be activated under this section in any twelve (12) month period, unless the audit is following upon a Personal Data Breach caused by TMF in the same period. Any further Data Protection Audit shall be at the Client's expense.

The Client's requests provided in this section 7 will be fulfilled in close co-operation with and under supervision of TMF's Chief Security and Resilience Officer, TMF's Chief Privacy Officer, or similar TMF local officials.

8. DELETION OR RETURN OF CLIENT PERSONAL DATA

TMF will, at the choice of the Client, delete or return the Personal Data at the end of the provision of the Services relating to Processing, unless (i) Data Protection Laws, (ii) any law, statute, order, regulation, rule, requirement, practice and guidelines of any government, regulatory authority or self-regulating organization that applies to the Services in the country where those Services are being provided, or (iii) competent court, supervisory or regulatory body, require the retention of such Personal Data by TMF.

9. INCIDENT MANAGEMENT

TMF shall notify the Client without undue delay after becoming aware of a Personal Data Breach, providing the Client with sufficient information which allows the Client to meet any obligations to report a Personal Data Breach under Data Protection Laws. Upon request by the Client, TMF shall fully co-operate with the Client and take such reasonable steps as are directed by the Client to assist in the investigation, mitigation and remediation of each Personal Data Breach, in order to enable the Client to (i) perform a thorough investigation into the Personal Data Breach and provide incident details as required under Data Protection Laws such as Article 33 (3) GDPR, (ii) formulate a correct response and (iii) take suitable further steps in respect of the Personal Data breach in order to meet any requirement under the Data Protection Laws ("**Remediation Measures**"). If TMF or TMF Affiliate has caused the Personal Data Breach, TMF shall bear the reasonable costs of the Remediation Measures taken by TMF. If and to the extent costs incurred by TMF related to the Remediation Measures as directed by the Client are related to the Personal Data breach

caused by the Client, the Client shall compensate reasonable costs of the Remediation Measures taken by TMF. Any costs borne by TMF that exceed to those reasonable costs for Remediation Measures shall be mutually agreed by the Parties in advance. The Remediation Measures shall: (i) start without undue delay, (ii) be completed within a reasonable period after TMF has become aware of a Personal Data breach, and (iii) be carried out within the regular business hours of the local office where the Remediation Measures are required to be taken.

10. INTERNATIONAL TRANSFERS OF — CLIENT PERSONAL DATA

Always subject to section 4 of this Policy and in the event the Services require international transfers of Personal Data between TMF, TMF Affiliate(s) and/or any Subprocessor(s), the following shall apply (insofar relevant):

- a. **Transfer to TMF Affiliates in or from EU.** The Personal Data may be transferred to (i) one or more of TMF's Affiliates in either one or more Member States of the European Economic Area ("EEA") or Switzerland on the basis of Data Protection Laws, or to (ii) one or more of the TMF's Affiliates in one or more third countries on the basis of the [Binding Corporate Rules](https://www.tmf-group.com/en/legal/data-protection/), which are published on the website of TMF Group (<https://www.tmf-group.com/en/legal/data-protection/>). The Client or the relevant TMF Affiliate shall upon request of the Client Data Subject, provide the Client Data Subject with a copy of such Binding Corporate Rules and this Policy (without any business sensitive or confidential information). Where permitted by Data Protection Laws, TMF shall obtain all relevant authorizations or permits for such transfer of Personal Data based on such Binding Corporate Rules. Where Data Protection Laws do not allow TMF to obtain such authorization or permit for itself, the Client shall in a timely manner issue a required authorisation to the relevant TMF Affiliate.
- b. **Transfer to Subprocessors in or from EU.** The Personal Data may be transferred (i) to one or more Subprocessors (other than TMF's Affiliates) in one or more Member States of the EEA or Switzerland on the basis of Data Protection Laws pursuant to the Clients permission ex section 5 of this Policy, or (ii) to one or more such Subprocessors in one or more third countries on the basis of an exception under Data Protection Laws, or (iii) on the basis of adequate safeguards added either, insofar as allowed under Data Protection Laws, by TMF to ensure the

protection of the Personal Data, or by the Client, in which case TMF shall cooperate with the Client to seek an adequate basis for the cross-border transfer of Personal Data to such Subprocessor. At the Client's request, TMF shall inform the Client of the applicable basis for the cross-transfer of the Personal Data.

- c. **Other transfers.** Where the data protection or privacy law of any country outside the EEA or Switzerland applies to the Personal Data, the Client shall ensure that any cross-border transfer of Personal Data from TMF to a Subprocessor shall be allowed, by implementing additional safeguards pursuant to Data Protection Laws or as otherwise permitted by Data Protection Laws.

11. LIABILITY

The Client warrants that all Personal Data processed by TMF on behalf of the Client has been and shall be Processed by the Client in accordance with Data Protection Laws including without limitation: (a) ensuring that all notifications to and approvals from regulators which are required by Data Protection Laws are made and maintained by the Client; and (b) ensuring that all Personal Data is Processed fairly and lawfully, is accurate and up to date and that a fair notice is provided to Client Data Subjects which described the processing to be undertaken by TMF pursuant to the Services agreed upon in the Service Agreement.

TMF shall be liable for the damage caused by Processing only where it has not complied with obligations of Data Protection Laws specifically directed to processors or where it has acted outside or contrary to lawful instructions of the Client as indicated in the Service Agreement. Client shall be liable for the damage caused by Processing by Client which infringes Data Protection Laws. Client or Processor shall be exempt from liability under this section 11 if it proves that it is not in any way responsible for the event giving rise to the damage.

Where more than one Controller or Processor, or both a Controller and a Processor, are involved in the same processing and where they are, under the Service Agreement, responsible for any damage caused to Client Data Subject by Processing, each Controller or Processor shall be held liable for the entire damage in order to ensure effective compensation of the Client Data Subject(s). Where a Controller or Processor has paid full compensation for the damage suffered, that Controller or Processor shall be entitled to claim back from the other Controller(s) or Processor(s) involved in the same Processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in the previous paragraph.



Save for this section 11 third paragraph, the indemnities, liabilities and exclusions or limitations thereof set out in the Service Agreement, shall also apply to the obligations of the parties pursuant to this Policy and the Service Agreement, and in case of any conflict will prevail.

12. CONTACT US

If you have any queries about this Policy or about the privacy practices of TMF Group, please send an email to dataprotection@tmf-group.com and be sure to indicate the nature of your query.

REFERENCE TO ASSOCIATED DOCUMENTS

RELATED DOCUMENTS	
Statement of Continuity	Latest version available on the website of TMF Group
Binding Corporate Rules	Latest version available on the website of TMF Group

REVISION HISTORY AND RECORDS

VERSION	DATE	AUTHOR	DETAILS
1.0	01-03-2018	Chief Privacy Officer	First version approved.
2.0	29-04-2019	Chief Privacy Officer	Sections 1, 3, 6, 7, 9, 10 and 11 revised to clarify TMF Group Personal Data Processing role and duties.
2.1	24-01-2020	Chief Privacy Officer	Sections 3 and 5 revised to include the details of processing and the list of Subprocessors links.
2.2	29-03-2020	Chief Privacy Officer	General Notice updated to accommodate organisational changes. Section 5 revised to clarify possible TMF Affiliate role as a Subprocessor. Sections 7 updated due to an organisational change.
2.3	03-06-2021	Group Privacy Office	Section 1 revised to clarify applicable version of Policy to the Services Agreement, as well as amendments required by law. Section 2 updated to include definitions for “Data Protection Audit” and “Personal Data Breach”. Section 5 revised to increase number of days for controller to object to appointment of new subprocessor(s) and clarifying language for potential resolutions upon objection. Section 6 revised to clarify application of further versions of the Statement of Continuity. Section 7 revised language to clarify obligations under data protection laws, inclusion of new defined terms and update due to organisational change. Section 9 updated to include allocation of costs for personal data breaches caused by TMF